

e-Commerce Fraud

Prevention, Detection, Legal Aspects, and the Role of Crime-as-a-Service

DIPLOMARBEIT

zur Erlangung des akademischen Grades

Diplom-Ingenieur

im Rahmen des Studiums

Business Informatics

eingereicht von

Thomas Ebner, Bakk.rer.soc.oec.

Matrikelnummer 0726345

an der Fakultät für Informatik

der Technischen Universität Wien

Betreuung: Ao. Univ.-Prof. Mag. Dr. iur. Markus Haslinger

Wien, 23. April 2018

Thomas Ebner

Markus Haslinger

e-Commerce Fraud

Prevention, Detection, Legal Aspects, and the Role of Crime-as-a-Service

DIPLOMA THESIS

submitted in partial fulfillment of the requirements for the degree of

Diplom-Ingenieur

in

Business Informatics

by

Thomas Ebner, Bakk.rer.soc.oec.

Registration Number 0726345

to the Faculty of Informatics

at the TU Wien

Advisor: Ao. Univ.-Prof. Mag. Dr. iur. Markus Haslinger

Vienna, 23rd April, 2018

Thomas Ebner

Markus Haslinger

Declaration of Authorship

Thomas Ebner, Bakk.rer.soc.oec.
Talgasse 4/27, 1150 Vienna

I hereby declare that I have written this Diploma Thesis independently, that I have completely specified the utilized sources and resources and that I have definitely marked all parts of the work - including tables, maps and figures - which belong to other works or to the internet, literally or extracted, by referencing the source as borrowed.

Vienna, 23rd April, 2018

Thomas Ebner

Acknowledgements & Dedications

I would like to express my gratitude to those who were involved in the creation of this thesis:

First and foremost, I would like to thank Prof. Dr. Haslinger for supervising my thesis, the guidance, continuous support, and the valuable feedback.

Furthermore, I would like to thank all interviewed experts who shared their knowledge and expertise, and contributed valuable information and insights to the success of the thesis.

Last, but definitely not least, I would like to thank Katrin for sparking my interest in the topic of e-commerce fraud, our subject-specific discussions and exchange, and for your highly appreciated support throughout the process of writing my thesis.

I dedicate this thesis to my parents, Monika and Chrysanth, even though neither this dedication nor words can express how grateful I really am. Thank you for your unconditional support and for everything you did and have made possible for me.

I also dedicate this thesis to my brother, Daniel. Thank you for everything you did for me, for always being there for me, and - quoting him as there are no better words to express it - “for accompanying me all my life and some nine months more, and for proving that brothers can be friends too”.

Abstract

E-commerce has become a self-evident part of our everyday life over the last few years, and its importance continues to grow. However, the success comes at a price: Not only has the volume of e-commerce transactions grown, but also the volume of fraudulent e-commerce transactions has increased in parallel too, at an even greater rate. Fraudsters are trying hard to emulate legitimate behaviour and behave like genuine customers, which tricks retailers and causes not only financial damage.

The thesis at hand is focused on B2C e-commerce fraud. The relevance and impact of e-commerce fraud is highlighted, and indicators for fraudulent e-commerce transactions are determined. Moreover, e-commerce transactions are analysed, and their vulnerabilities and their susceptibility with regard to fraud attempts are investigated and evaluated. Measures to prevent and to detect e-commerce fraud are gathered and analysed as well. Interviews with investigators and experts in this field are conducted to gain practical insights, and to enhance the knowledge and discuss the results acquired from the literature research.

Furthermore, legal aspects with regard to e-commerce fraud are examined. This comprises an analysis of the Austrian legislation as well as international endeavours against e-commerce fraud (with an impact on Austrian laws), as e-commerce (and, consequently, e-commerce fraud) is inherently cross-border.

Another factor contributes to the rise of e-commerce fraud as well: Over the last few years, cybercriminals have advanced to profit- and service-oriented business models, leading to a phenomenon referred to as Crime-as-a-Service. Cybercriminals provide their goods and services to other criminals, which is why the entry barrier is diminished, making it easier for criminals to commit crimes like e-commerce fraud. An investigative research of the relevance and impact of Crime-as-a-Service on e-commerce fraud and its facilitating role is also included in the present thesis.

Kurzfassung

Im Laufe der letzten Jahre hat sich E-Commerce zu einem festen Bestandteil unseres täglichen Lebens entwickelt, und die Bedeutung wird weiter steigen. Der Erfolg hat aber auch seine Schattenseite: Während einerseits das Volumen an E-Commerce Transaktionen zunimmt, steigt andererseits zugleich auch der Anteil an Betrugsfällen, sogar in einem noch höheren Ausmaß. Betrüger treten als vertrauenswürdige Kunden auf, und verursachen den dadurch getäuschten Online-Händlern nicht nur finanziellen Schaden.

Die Diplomarbeit beschäftigt sich mit E-Commerce Betrug im B2C-Bereich, also mit E-Commerce Transaktionen zwischen betrügerischen Endkunden und Online-Händlern. Die Bedeutung und die Auswirkung von E-Commerce Betrug wird aufgezeigt und Indikatoren für betrügerische Transaktionen ermittelt. Der Ablauf von E-Commerce Transaktionen wird analysiert; dargelegte Schwachstellen werden hinsichtlich ihrer Anfälligkeit für betrügerische Aktivitäten untersucht und evaluiert. Zudem werden Maßnahmen zur Vermeidung und zur Erkennung von Betrugsversuchen analysiert. Interviews mit Ermittlern und Experten im Bereich E-Commerce Betrug werden durchgeführt, um so Informationen aus der Praxis zu erhalten, und um das in der Literaturrecherche gesammelte Wissen zu erweitern und zu evaluieren.

Darüber hinaus werden auch die rechtlichen Aspekte hinsichtlich E-Commerce Betrug untersucht. Dies umfasst eine Analyse der österreichischen Gesetzeslage als auch internationaler Bemühungen gegen E-Commerce Betrug, welche Auswirkungen auf die österreichische Gesetzgebung haben, da E-Commerce (und somit auch E-Commerce Betrug) von Natur aus länderübergreifend ist.

Ein weiterer Faktor trägt zum Anstieg von E-Commerce Betrug bei: Über die letzten Jahre haben sich Cyberkriminelle profit- und serviceorientierten Geschäftsmodellen zugewandt, was zur Entstehung des sog. Crime-as-a-Service (etwa: Verbrechen als Dienstleistung) geführt hat. Cyberkriminelle stellen ihre (zumeist illegalen) Güter und Dienstleistungen anderen Cyberkriminellen zur Verfügung, was dazu führt, dass für diese die Einstiegsbarriere gesenkt wird, wodurch es einfacher wird kriminelle Machenschaften, wie etwa E-Commerce Betrug, zu begehen. Eine investigative Recherche hinsichtlich der Bedeutung und der Auswirkung von Crime-as-a-Service auf E-Commerce Betrug ist ebenso Teil dieser Diplomarbeit.

Contents

1	Introduction	3
1.1	Motivation and problem definition	3
1.2	Expected results	5
1.3	Methodological approach	6
1.4	Structure of the work	7
2	E-commerce	9
2.1	Definition of e-commerce	9
2.2	Relevance of e-commerce	10
2.3	Categories of e-commerce	11
2.4	E-commerce transaction: Processes and stakeholders	13
2.4.1	Agreement	13
2.4.2	Payment	14
2.4.3	Delivery	15
2.5	Online payment	16
2.5.1	Online payment methods	16
3	E-commerce fraud	23
3.1	Definition of e-commerce fraud	23
3.1.1	1 st vs. 3 rd party e-commerce fraud	25
3.2	Relevance and impact of e-commerce fraud	26
3.2.1	Impact on consumers	27
3.2.2	Impact on merchants	28
3.2.3	Impact on payment facilities	29
3.3	Anatomy of e-commerce fraud	29
3.3.1	Agreement	29
3.3.2	Payment	31
3.3.3	Delivery	37
3.4	Indicators of e-commerce fraud	41
3.4.1	Agreement	42
3.4.2	Payment	43
3.4.3	Delivery	44

4	Preventing e-commerce fraud	47
4.1	General	47
4.2	Collection and analysis of fraudulent transactions and attempts	47
4.3	Measures for identity verification	48
4.3.1	Data verification	49
4.3.2	ID check	50
4.3.3	Trusted virtual identity	50
4.4	Security measures provided by payment methods	51
4.5	Restriction of payment methods	53
4.6	Restrictions and security measures for delivery services	54
5	Detecting e-commerce fraud	57
5.1	General	57
5.1.1	Transaction scoring	59
5.1.2	Costs	60
5.1.3	Challenges	60
5.2	Manual review	64
5.3	Information provider	64
5.3.1	Data verification provider	65
5.3.2	Credit score provider	65
5.3.3	Information sharing provider	66
5.4	Data analysis	66
5.4.1	Rule-based expert methods	67
5.4.2	Supervised classification methods	68
5.4.3	Unsupervised anomaly detection methods	71
6	Legal aspects and prosecution of e-commerce fraud	73
6.1	Legislation in Austria	73
6.1.1	Legal assessment of the contractual relationship	73
6.1.2	Criminal offences	76
6.1.3	Jurisdiction and venue	91
6.2	Transnational endeavours against fraud	94
6.2.1	Convention on Cybercrime (Council of Europe)	94
6.2.2	Framework Decision on combating fraud (European Union)	98
7	Crime-as-a-Service	101
7.1	Cybercrime and the emergence of Crime-as-a-Service	101
7.1.1	As-a-Service business models facilitating e-commerce fraud	105
7.2	Facilitating factors of Crime-as-a-Service	110
7.2.1	Anonymisation	110
7.2.2	Forums	115
7.2.3	Communication	117
7.2.4	Marketplaces	119
7.2.5	Cryptocurrencies	121

7.2.6	Online disinhibition effect	123
7.3	Measures against Crime-as-a-Service	125
7.4	Challenges of law enforcement	127
8	Investigative research in the Crime-as-a-Service economy	131
8.1	Objectives and procedure	131
8.2	Prerequisites and preparation	134
8.3	Investigation	135
8.3.1	Forums	135
8.3.2	Marketplaces	137
8.3.3	Shops	138
8.3.4	Other hidden services	139
8.4	Summary	139
9	Conclusion	143
A	Expert interviews	147
A.1	General	147
A.2	Interviews with investigators	149
A.2.1	Focus areas of the interviews	149
A.2.2	Investigator of Europol	150
A.2.3	Investigator of Criminal Intelligence Service Austria	154
A.3	Interview with expert from payment provider	159
A.3.1	Focus areas of the interview	159
A.3.2	Payment provider for payment after delivery	160
A.4	Interviews with merchants	163
A.4.1	Focus areas of the interviews	163
A.4.2	Merchant #1	164
A.4.3	Merchant #2	167
B	Investigation in the Darknet	169
B.1	Addresses of hidden service	169
B.1.1	Search engines	169
B.1.2	Directories	169
B.1.3	Forums	170
B.1.4	Marketplaces	171
B.1.5	Shops	171
B.1.6	Other hidden services	172
B.2	Screenshots	173
C	Abbreviations	193
	List of Figures	195
	List of Tables	197

“Fraud is the daughter of greed.”

Jonathan Gash

Introduction

1.1 Motivation and problem definition

Electronic commerce¹, commonly abbreviated to e-commerce, has already become a self-evident part of our everyday life. It started its race to success with the rise of the Internet, and is expected to continue the run. In 2016 alone, 58% of the Austrian population has purchased goods or services online.² The numbers become even more impressive on a larger scale. In Europe, the third-largest e-commerce market after Asia-Pacific and North America, the revenue of e-commerce sums up to 505 billion US dollars in 2015.³ An estimated 1.6 billion people worldwide shop online, and within the next five years the number is expected to increase up to 2.3 billion people.⁴ Moreover, the estimated worldwide e-commerce revenue in 2015 is 2.3 trillion US dollars.⁵ The huge development and spread of the mobile market, which connects more and more users to the Internet, and the progressing globalization, which impacts the increasing volume of cross-border transactions, add to this as well.

However, the increasing success of e-commerce is also reflected in the increase in e-commerce fraud. Current numbers show that attacked e-commerce transactions, i.e. transactions that were subject to successful or unsuccessful fraud attempts, increased from 0.9% at the beginning of 2015 to up to 3.9% in the middle of 2016.⁶ The potential fraud costs, i.e. the money a merchant loses if each transaction subject to fraud is successful, quadrupled from 2 to 8 US dollars out of every 100 US dollars in the same

¹The term “electronic commerce” summarizes all kind of businesses that are conducted via electronic means (predominantly via the Internet); the focus of this work is on retail business (B2C) only.

²[1].

³[2].

⁴[3].

⁵[2].

⁶[4], p.15.

time frame.⁷ A recent survey among e-commerce companies in Austria, Germany and Switzerland has shown that almost every participating merchant has already been victim to e-commerce fraud.⁸

E-Commerce companies are confronted with an increasing volume of transactions and, as a consequence thereof, with more cases of fraud. Thus, the effort and the costs to prevent and to detect fraudulent transactions are also increasing. Fraudsters are trying hard to always be a step ahead of e-commerce companies and perfect the ways in which they emulate the legitimate behaviour of a trustworthy customer.⁹ It is increasingly difficult for e-commerce companies to prevent and detect fraud. Furthermore, they have to walk a fine line between optimizing the customer's experience and customer satisfaction, while still taking measures against e-commerce fraud.¹⁰ While customers are demanding fast and frictionless online shopping experiences, it counteracts the efforts to detect and prevent e-commerce fraud.¹¹

A particularity regarding e-commerce fraud is that the exchange of information within this field is limited and usually not made available to the public.¹² While the concerns are of course valid, it also makes it more difficult to spread knowledge about the various techniques and strategies used by fraudsters, and it makes the development of measures against fraud, such as fraud detection methods, more complicated.¹³ On the contrary, fraudsters share and trade information in underground communities about how to commit e-commerce fraud, share tried and tested strategies and security breaches, and form networks and organize themselves in crime groups.¹⁴

Not only has e-commerce become a big business over the last years, cybercrime has also evolved and has become a big business in itself. Criminal organizations and networks with hierarchies, specialized roles, as well as profit- and service-oriented business models emerged that offer their criminal services to other criminals. This phenomenon is termed as *Crime-as-a-Service*.¹⁵ The rise of Crime-as-a-Service has also had an impact on e-commerce fraud. Criminals can procure the products and services of highly skilled criminals, which is why the entry barrier, especially with regard to technical skills, has diminished.¹⁶ As stated by Europol, Crime-as-a-Service “*grants easy access to criminal products and services, enables a broad base of unskilled, entry-level cybercriminals to launch attacks of a scale and scope disproportionate to their technical capability and asymmetric in terms of risks, costs and profits*”¹⁷.

⁷[4], p.8.

⁸[5].

⁹[6].

¹⁰[6].

¹¹[6].

¹²[7], p.384.

¹³[7], p.384.

¹⁴[8], p.70.

¹⁵[9], pp.9–10.

¹⁶[10], p.98.

¹⁷[11], p.7.

Despite these developments, a survey conducted in Germany in 2015 showed that one quarter of the participating companies (mostly small and medium-sized businesses) don't take any precautions against e-commerce fraud at all.¹⁸ Among the main arguments as to why they don't have any counter-measures were due to limited resources (both personnel-wise and financial), no knowledge about counter-measure options, and bad cost-benefit ratio.¹⁹ The other three quarters of the participating companies often perform manual checks to validate a transaction, which are costly and time-consuming, or use credit rating services from external service providers.²⁰ While large businesses usually have the resources to fight fraud (for example, by employing experts or installing anti-fraud systems), smaller businesses often lack the expertise and the resources for counter-measures against e-commerce fraud, making it "*a significant contributing factor to small business failure*"²¹.

Summarizing these trends, the number of e-commerce transactions is continuing to increase, while the number of e-commerce fraud attempts increases even more. Fraudsters not only strive to find and exploit new ways to commit e-commerce fraud, they and their techniques, respectively, are becoming increasingly more professional and organized, mainly due to the facilitating role of Crime-as-a-Service. Merchants are therefore confronted with a growing threat and increasing costs to brace themselves against e-commerce fraud attempts. The increasing costs and often limited resources, especially that of small and medium sized companies, pose a significant and often overpowering problem for merchants. By not reacting to these trends, merchants risk not only severe financial losses but also face the risk of bankruptcy.

1.2 Expected results

The objective of the present thesis is to provide an in-depth overview of the growing threat of e-commerce fraud and topics closely related to it. The current situation of e-commerce fraud and the vulnerabilities of e-commerce transactions are analysed and indicators for e-commerce fraud are determined. Counter-measures to prevent and detect e-commerce fraud are gathered and evaluated, and effective solutions are highlighted. The aim is to give a clear picture of the threat of e-commerce fraud and how to effectively respond to it.

Additionally, a legal analysis is conducted to provide an overview of the legal situation, not only within the legal framework of Austria, but with regards to international endeavours against e-commerce fraud (due to the inherent cross-border character of e-commerce transactions).

Moreover, it is investigated how Crime-as-a-Service facilitates e-commerce fraud and contributes to the increase of fraud attempts targeting e-commerce transactions.

¹⁸[12], p.25.

¹⁹[12], p.33.

²⁰[12], p.28.

²¹[13], p.13.

The expected results of the thesis at hand are closely related to the following research questions:

- (1) What are the characteristics of e-commerce fraud?
 - (1a) What are measures to prevent e-commerce fraud?
 - (1b) What are measures to detect e-commerce fraud?
- (2) What are the legal aspects of e-commerce fraud?
- (3) How does Crime-as-a-Service facilitate e-commerce fraud?

1.3 Methodological approach

The methodological approach comprises the following steps:

1. Literature research

Comprehensive research and analysis of scientific and subject-specific literature, company publications and online resources are conducted to gain an in-depth overview of e-commerce fraud and related topics addressed by the research questions.

2. Legal analysis

For the legal part of the thesis, legislative texts from the Austrian law regarding e-commerce fraud are analysed. Since e-commerce fraud is in most cases a cross-border crime, international endeavours with an impact on the legislation in Austria are analysed as well. The result of this analysis clarifies the legal situation regarding e-commerce fraud and also highlights the legal limitations and challenges, especially with regard to cross-border crimes.

3. Qualitative research

This part of the thesis is concerned with exploring the topics addressed by the research questions with experts from practice as well as conducting investigative research to gain more insights into the impact of e-commerce fraud, the measures to respond to it, and the associated challenges. The following two methods are used:

a) Interviews with experts in the field of e-commerce fraud

To gain practical insights and information about e-commerce fraud and related topics addressed by the research questions, interviews are conducted with experts in the field of e-commerce fraud. The experts are from three different areas: (a) Investigators from Europol and the Criminal Intelligence Service Austria, (b) Fraud experts of payment providers, and (c) Fraud experts of merchants. Additionally, the counter-measures against fraud which are gathered in the literature research are evaluated and their practical applicability and advantages are discussed with the interviewees.

b) Investigative research

Investigative research is conducted in the cybercrime community. The objective is to find out how Crime-as-a-Service facilitates e-commerce fraud, and how complex it is for fraudsters to make use of the services and products provided by the underground economy to commit e-commerce fraud.

1.4 Structure of the work

Chapter 2 contains the fundamentals of e-commerce and relevant information regarding e-commerce fraud. This is followed by a chapter on e-commerce fraud, where terminology is defined and the impact of e-commerce fraud is highlighted. Moreover, the anatomy of e-commerce transactions and their vulnerabilities regarding fraud are analysed and evaluated, and indicators for e-commerce fraud are determined. In chapter 4, measures to prevent e-commerce fraud are gathered, while chapter 5 is concerned with measures to detect fraudulent e-commerce transactions. Chapter 6 is dedicated to legal aspects related to e-commerce fraud. A comprehensive overview about Crime-as-a-Service is given in chapter 7. Furthermore, chapter 8 describes the investigative research in the cybercrime community to assess the facilitating role of Crime-as-a-Service regarding e-commerce fraud.

The thesis is concluded with chapter 9: The results of the preceding chapters and the insights of the interviews and the investigative research are discussed.

In the appendix, the interviews with investigators and fraud experts are summarized.

E-commerce

2.1 Definition of e-commerce

E-commerce (short for *electronic commerce*) is, broadly speaking, commerce (from Latin *commercium*: trade, trading¹) conducted via electronic connections in the form of transactions.^{2,3} A transaction is “*the exchange of goods or services between a buyer and a seller*”⁴. E-commerce, therefore, refers to “*the use of electronic means and technologies to conduct commerce (sale, purchase, transfer, or exchange of products, services and/or information)*”⁵.

The difference between (traditional) commerce and e-commerce can be illustrated using the framework proposed by *Choi et al.* (cf. figure 2.1). The framework is based on three dimensions: *Product*, *Process*, and *Delivery Agent*.⁶ For each dimension, it is differentiated if a transaction is either *physical* or *digital*.⁷ If a transaction is categorized as *physical* in all three dimensions, it is categorized as *traditional commerce*.⁸ In addition, if all of the three dimensions of a transaction are *digital*, it is categorized as *core e-commerce*.⁹ All other scenarios, i.e. if there is at least one dimension considered as digital for a transaction, are categorized as *partial e-commerce*.¹⁰

¹[14].

²[15], p.2.

³[16], p.15.

⁴[17], p.23.

⁵[18], p.2.

⁶[18], p.4.

⁷[16], p.17.

⁸[16], p.18.

⁹[16], p.18.

¹⁰[18], p.4.

¹¹Reprinted from [18], p.4.

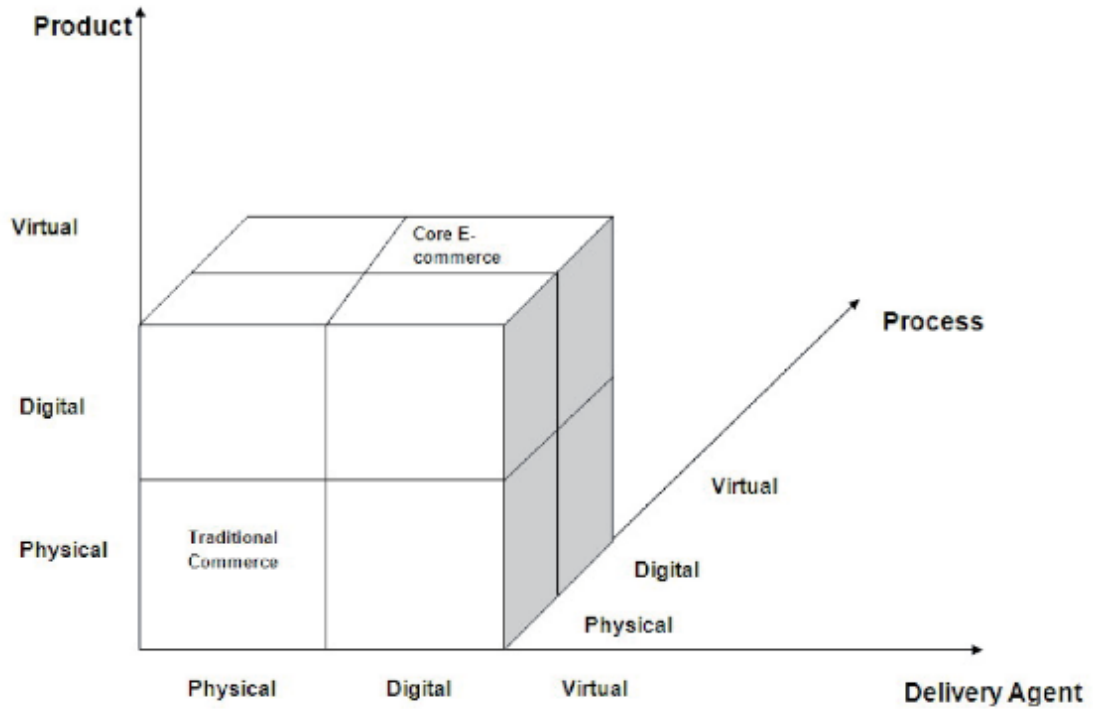


Figure 2.1: E-commerce framework¹¹

2.2 Relevance of e-commerce

Table 2.1 shows an overview of global B2C e-commerce figures^{12,13}:

The region with the highest revenue is Asia-Pacific, followed by North America and Europe. Far behind are Latin America, MENA (Middle Eastern and North Africa), and the rest of the world (aggregated as Others). Although the average spending of online shoppers from the Asia-Pacific region is lower than those from North America and Europe (1,582 US\$ vs. 3,099 US\$ and 1,709 US\$), and despite a lower rate of online shopping (22% vs. 54% and 43%), Asia-Pacific accounts for nearly half of the global B2C e-commerce revenue due to its massive population. In total, every second online shopper is from the Asia-Pacific region.

The higher revenue of North America compared to Europe is all the more remarkable when comparing the numbers. While the rate of Internet consumption is almost the same (77% vs. 75%), the number of Internet users is much lower in North America (298mn vs. 516mn). However, the rate of online shopping is much higher in North America (54% vs. 43%), and the average spending is nearly twice as high (3,099 US\$ vs. 1,709 US\$).

¹²[2].

¹³[19].

Although B2C e-commerce sales are still a fraction of the gross global retail sales, approximately 8.7% in 2016, the total value is nonetheless formidable: The worldwide total value of B2C e-commerce sales in 2015 was 2.27 trillion US dollars, and is projected to increase within the next five years to a ratio of around 14.6%.

Region	Revenue (in US\$)	Growth rate (in %)	Internet users	Online buyers	Average spending (in US\$)
<i>World</i>	2,273bn	+19.9%	2,521mn (45%)	1,437mn (26%)	1,582
Asia-Pacific	1,057bn	+28%	1,223mn (39%)	711mn (22%)	1,486
North America	644bn	+12.5%	298mn (77%)	208mn (54%)	3,099
Europe	505bn	+13.3%	516mn (75%)	296mn (43%)	1,709
Latin America	33bn	+28%	221mn (56%)	94mn (24%)	352
MENA	26bn	+19%	148mn (38%)	82mn (21%)	313
Others	8bn	+23%	115mn (21%)	46mn (8%)	174

Table 2.1: Global B2C e-commerce figures (2015)¹⁴

2.3 Categories of e-commerce

Based on the entities participating in an e-commerce transaction, and the type of the transaction itself, distinct categories are differentiated. The participating entities in e-commerce are *Business*, *Consumer*¹⁵, and *Government*^{16, 17, 18}. Some sources also classify the entity *Employee*, but it can be argued that this entity is in fact a special type of consumer.¹⁹

An e-commerce transaction always consists of two entities: one entity acts as a supplier of a good or service, and the other entity as a consumer.²⁰ Each of the listed entities can either be a supplier or a consumer in a transaction; an entity can, therefore, participate

¹⁴[2].

¹⁵The literature also uses the terms *Customer* or *Client*. In this context, these terms have the same meaning and can be used interchangeably. In case of governmental involvement, the term *Citizen* is preferably used.

¹⁶The term *Administration* is also used in the literature.

¹⁷[20], pp.26–27.

¹⁸[18], pp.5–8.

¹⁹[20], p.27.

²⁰[20], p.26.

in multiple categories depending on the nature of the transaction.²¹ Combining these entities results in nine e-commerce categories as shown in table 2.2.^{22,23}

		Supplier		
		B	C	G
Consumer	B	B2B	C2B	G2B
	C	B2C	C2C	G2C
	G	B2G	C2G	G2G

Table 2.2: Categories of e-commerce

In the following, the e-commerce categories are explained briefly:

- **B2B - Business-to-Business**^{24,25}: B2B e-commerce are transactions between companies. This category is also known as *e-procurement* since businesses procure goods and services from other businesses. Today, most of the transactions in e-commerce belong to this category.
- **B2C - Business-to-Consumer**^{26,27}: The relationship in this category is between a business and a consumer. A company provides goods or services, which can be purchased by the general public. Since these companies are usually retailers, this category is also called *e-retailing* or *e-tailing*. It is the second largest category of e-commerce.
- **B2G - Business-to-Government**^{28,29}: E-commerce is used by governments and governmental organizations for public procurement. Purchasing demands are made available publicly. Businesses can offer their goods and services, and the government or governmental organization can select an offer.
- **C2B - Consumer-to-Business**^{30,31}: In this category, which can be seen as inverted B2C e-commerce, a transaction is initiated by a consumer. Consumers

²¹[21], p.6.

²²[21], pp.6–9.

²³[20], pp.26–27.

²⁴[18], p.5.

²⁵[22], p.10.

²⁶[18], pp.5–6.

²⁷[23], pp.27–28.

²⁸[18], p.6.

²⁹[23], pp.30–32.

³⁰[18], pp.6–7.

³¹[22], p.11.

offer what they are willing to pay for a product or service, and businesses can decide if they want to provide it for the stated offer.

- **C2C - Consumer-to-Consumer**^{32,33}: Transactions happen between consumers. For this type of e-commerce, a third party is usually involved that enables the consumers to connect with each other and facilitates the transactions. Examples for C2C e-commerce are auction sites or platforms for second-hand goods. In addition, C2C transactions can also take place via social media.
- **C2G - Citizen-to-Government**³⁴: In theory, this category is for transactions between citizens and governments. In practice, it is not common that individuals provide services to governments or governmental institutions. Therefore, this category differs from the true nature of e-commerce, as it comprises transactions such as the payment of taxes.
- **G2B/C/G - Government-to-Business/Citizen/Government**^{35,36}: As with the category above, these categories are non-commercial. They comprise of transactions between governments or governmental organizations and businesses/citizens/governments from other nations or governmental organizations within one nation or between nations. The underlying purpose is information dissemination as well as providing services, assistance and support.

2.4 E-commerce transaction: Processes and stakeholders

An e-commerce transaction consists of three processes: *Agreement*, *Payment*, and *Delivery*.³⁷

2.4.1 Agreement

Two stakeholders are involved in this process: a *Consumer* and a *Merchant*.³⁸ The minimal determination comprises the goods or services and the price that has to be paid for them.³⁹

Consumer

Consumers have the intent to purchase goods or services from merchants.⁴⁰

³²[18], p.7.

³³[23], pp.36–39.

³⁴[24], p.373.

³⁵[18], pp.7–8.

³⁶[22], p.11.

³⁷[25], pp.219–220.

³⁸[25], p.219.

³⁹[25], p.219.

⁴⁰[26], p.54.

Merchant

Merchants are offering goods and services to consumers.⁴¹ It is common that merchants outsource parts of an e-commerce transaction to third parties that are more specialized, effective and efficient in handling certain tasks such as payments (cf. *Payment Service Provider*) or logistic services (cf. *Logistics Service Provider*).

2.4.2 Payment

In this process of an e-commerce transaction, the consumer and the merchant agree on how the order is paid.⁴² In most cases, a third stakeholder is involved to handle the payment: a *Payment Service Provider*.⁴³ The selected payment method affects the transaction and the involved stakeholders. First, the payment can be carried out either online or offline; in the case of the former, the payment can either be integrated in the purchasing process, or can take place before or after the delivery.^{44,45} Second, additional stakeholders might get involved which are necessary to ensure that the money is withdrawn from the customer and credited to the merchant.⁴⁶

Payment Service Provider

Payment Service Providers (PSPs) allow merchants to accept payments from their consumers online by handling their payments. To understand how a payment is handled, it must be distinguished between *Payment Service Provider*, *Payment Processor*, and *Payment Gateway*^{47,48,49,50}:

The *Payment Gateway* acts as an intermediary between an online shop and the payment processor. Due to security reasons, it is not allowed that transaction details are directly transmitted from an online shop to the payment processor. Therefore, the payment gateway acts as a mediator and ensures the encryption and security of transaction details.

The *Payment Processor* executes the transaction, i.e. receives the transaction details from the payment gateway and communicates with parties required for the payment (e.g. banks or payment networks) to execute the transaction. While it is not mandatory to use a payment processor, the advantage is that they already provide the physical infrastructure for communication with required parties (if only a payment gateway is used, the connection with each required parties must be contracted and established individually).

⁴¹ [27], p.2200.

⁴² [25], p.219.

⁴³ [28], pp.68–69.

⁴⁴ [29], pp.25–26.

⁴⁵ [28], pp.69–70.

⁴⁶ [28], pp.68–75.

⁴⁷ [30], pp.13–15.

⁴⁸ [30], pp.35–36.

⁴⁹ [31].

⁵⁰ [32].

Payment Service Providers can be seen as aggregators, as they combine payment processors and payment gateways, and act as a single point of service. This allows merchants to use multiple payment methods and local payment methods in different countries; consequently, their technical and administrative effort is reduced since the connection to required parties must not be established directly. Moreover, PSPs often offer additional services such as risk management or fraud prevention.

The three entities are not always completely independent of each other: for example, there are payment processors that provide their own payment gateway.⁵¹

2.4.3 Delivery

In this process of an e-commerce transaction, the customer and the merchant agree on how the order is delivered.⁵² If the purchased products are not virtual, i.e., intangible goods, the involvement of another stakeholder is required in this process of an e-commerce transaction: a *Logistics Service Provider*.⁵³

Logistics Service Provider

The delivery of tangible orders in most cases of B2C e-commerce is fulfilled by *Logistics Service Providers* (LSP), also termed as *Third Party Logistics* (3PL).⁵⁴ As the effective and efficient shipping of orders is critical for e-commerce companies, LSPs play an important role in e-commerce transactions.^{55,56}

LSPs are often not only providing shipment of orders from merchants to consumers, but offer additional services such as the handling of product returns, warehousing or packaging, and the handling of the goods.^{57,58}

In summary, a typical e-commerce transaction involves at least four stakeholders: *Consumer*, *Merchant*, *Payment Service Provider* and *Logistics Service Provider*. In figure 2.2, a schematic e-commerce transaction is depicted. For the sake of illustration, no specific payment method is used (the *Payment Service Provider* is used as abstraction), and the delivery is carried out by a *Logistic Service Provider*.

⁵¹[31].

⁵²[25], p.219.

⁵³[33], p.142.

⁵⁴[34], pp.337-338.

⁵⁵[35], pp.667.

⁵⁶[36], pp.203-206.

⁵⁷[34], p.338.

⁵⁸[35], p.661.

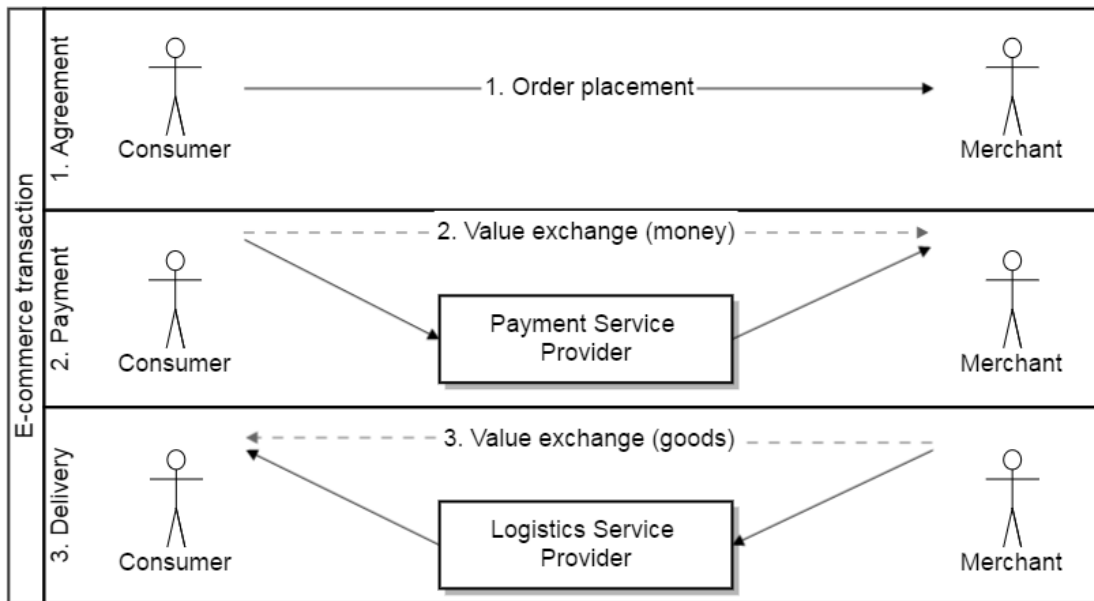


Figure 2.2: Schematic illustration of an e-commerce transaction

2.5 Online payment

A fundamental part of the value exchange between merchants and customers is the payment by a customer in order to settle the bill for the goods and services provided by a merchant.⁵⁹

Over the years, numerous online payment methods have emerged. While some are based on and have evolved from traditional payment methods (e.g. payment via credit card), others are solely enabled by the Internet (e.g. e-wallets).^{60,61}

2.5.1 Online payment methods

Table 2.3 shows the development regarding the top five online payment methods in recent years. Back in 2014, credit cards were predominantly used to pay online, and the gap to e-wallets and debit cards was noticeable.⁶² Nevertheless, within one year, e-wallets surpassed credit cards and are now the leading online payment method.⁶³ The rise of e-wallets are at the expense of credit cards and debit cards which lost considerable market shares.^{64,65} According to the forecast for 2020, e-wallet is still going to be the most used

⁵⁹[28], pp.68–70.

⁶⁰[37].

⁶¹[28], pp.68–70.

⁶²[38], p.13.

⁶³[39], p.6.

⁶⁴[38], p.13.

⁶⁵[39], p.6.

online payment method with a nearly constant share, while credit cards and debit cards will continue to lose market shares.⁶⁶

In 2014 and 2015, the top five online payments methods combined accounted for 90% of all online payments.^{67,68} The forecast shows that this coverage will slightly decrease over the next few years to 87%, while other payment methods are going to marginally increase their shares.⁶⁹ The three most used online payment methods are expected to decrease in market dominance : In 2015, e-wallets, credit cards and debit cards accounted for 73% of all online payments, which is predicted to decrease to 66% until 2020.⁷⁰

Online payment method	2014	2015	2020 (forecast)
Credit card	30%	25%	20%
Debit card	20%	17%	16%
e-Wallet	22%	31%	30%
Bank transfer	11%	10%	13%
Cash on delivery	7%	7%	8%
Coverage	90%	90%	87%

Table 2.3: Top five online payment methods in 2014, 2015, and 2020 (forecast)^{71,72}

For merchants, the following factors are of importance regarding the selection of appropriate online payment methods⁷³:

- **Regional support**⁷⁴: It is of relevance if an online payment method is supported and how effective it is in a certain region. While the support of a payment method is crucial, the effectiveness is based on the preferences of consumers in a certain region and the customer base.
- **Consumer preference**⁷⁵: It is not sufficient to select payment methods supported in a certain region, they also have to be accepted and used by the consumers.

⁶⁶[39], p.6.

⁶⁷[39], p.6.

⁶⁸[38], p.13.

⁶⁹[39], p.6.

⁷⁰[39], p.6.

⁷¹[38], p.13.

⁷²[39], p.6.

⁷³[30], p.4.

⁷⁴[30], p.5.

⁷⁵[30], p.5.

Preferences can be based on trust, ease of use, or market dominance, as well as historical preferences (for example, Germany is historically a catalogue order country, wherefore *Payment after delivery* is still one of the most preferred online payment methods.⁷⁶).

- **Customer base**⁷⁷: Not only should the online payment methods preferred by consumers be considered, the size of the customer base is equally as important. For this, the customer base should be divided into current and potential customers to ensure that online payment methods are selected to maximize the customer base.
- **Return on investment (ROI)**⁷⁸: Each online payment method bears varying costs, such as transaction or integration fees. Since it directly impacts the ROI, this must be considered as well when making a selection.

The various online payment methods are described below.

Credit card

Credit cards are issued to consumers with a certain line of credit, and can be used both offline and online.⁷⁹ They are widely used internationally and, therefore, have a high acceptance rate.⁸⁰ The spent amount of money is accumulated to the account of the card holder and is due at a later, pre-defined point in time.⁸¹

Debit card

The functionality of debit cards is similar to that for credit cards.⁸² In contrast to credit cards, the billed amount of money is withdrawn from the card holder's account as soon as the transaction is processed.⁸³ A prerequisite for a successful payment is the balance and overdraft facility; if the available funds are insufficient, the transaction is rejected.⁸⁴

Pre-paid card

A pre-paid card is handled and processed equally to that of a credit or debit card.⁸⁵ The difference is that in order to be able to make a payment, it must be preloaded with

⁷⁶[29], p.38.

⁷⁷[30], p.5.

⁷⁸[30], p.5.

⁷⁹[29], p.29.

⁸⁰[29], p.32.

⁸¹[29], p.29.

⁸²[29], p.33.

⁸³[28], p.70.

⁸⁴[39], p.90.

⁸⁵[29], p.33.

money in advance, and only the preloaded amount of money can be spent.⁸⁶ It is often used by people with bad credit history or for under-aged consumers.⁸⁷

Prepayment

There are different options for prepayments:

One option is the payment via bank transfer. After ordering a good or service, the consumer has to manually initiate the payment and transfer the money to the merchant's bank account.⁸⁸ For this, the consumer usually receives a reference number so that the merchant is able to connect the order with the respective payment.⁸⁹ The merchant continues the fulfilment process after the money is credited to the bank account. A disadvantage of this payment method is that the whole process is delayed until the payment is received by the merchant.⁹⁰

Another option is gift cards or vouchers.⁹¹ They have a certain value (depending on what has been paid in advance) and can be used as payment by entering the associated code. Due to the card's code, gift cards and vouchers can be virtual or tangible. Merchants often sell them directly, wherefore no PSP is required to make use of them.

Similar to gift cards, and not to be mixed up with pre-paid cards as described above, are pre-paid cards with associated codes.⁹² Like gift cards, the associated code must be entered to use it for a payment.⁹³ In contrast to gift cards, the issuance of these pre-paid cards and the processing is done by PSPs/PPs.⁹⁴

Electronic wallet

An electronic wallet, shortened to e-wallet, allows the use of various online payment methods, such as credit cards, debit cards, bank transfer, or gift cards with one e-wallet account.⁹⁵ Payments can be done either directly via linked payment methods, or the e-wallet can be preloaded with money.⁹⁶ The aggregation of various payment methods into one e-wallet simplifies and increases the convenience of online payments and improves the payment experience.⁹⁷ Additionally, e-wallets often provide further amenities such as additional consumer protection.⁹⁸

⁸⁶[29], p.33.

⁸⁷[39], p.90.

⁸⁸[39], p.88.

⁸⁹[39], p.88.

⁹⁰[39], p.88.

⁹¹[29], p.33.

⁹²[39], p.89.

⁹³[39], p.89.

⁹⁴[39], p.89.

⁹⁵[29], p.33.

⁹⁶[39], p.89.

⁹⁷[29], p.33.

⁹⁸[29], p.35.

Bank transfer

This online payment method allows the customer to complete a payment in real-time via bank transfer.⁹⁹ Consumers have to authenticate themselves and authorize the money transfer from their banking account to the banking account of the merchant.¹⁰⁰ Since money transfers between banks are not processed in real-time, the consumer's bank provides a guarantee to the merchant's bank.¹⁰¹ This allows the merchant to continue the fulfilment process, and the money arrives after a certain amount of time.¹⁰² A benefit of bank transfers is the relatively low transaction costs compared to other payment methods.¹⁰³

Direct debit

The consumer gives the merchant a mandate, either in paper or in electronic form, which authorizes the merchant to initiate the payment via bank transfer and withdraw the billing amount from the consumer's bank.¹⁰⁴ It is used for one-off and recurring payments (often used for subscriptions with recurring payment).¹⁰⁵

Payment after delivery

This payment method is also known as *Invoice* or *e-Invoice*.¹⁰⁶ Consumers receive their goods and, in case they want to keep it, they pay after the delivery within a defined time frame by initiating a bank transfer.¹⁰⁷ If they don't want to keep the product, they can return it without the need for a payment, and vice versa - if they don't pay, they have to return the goods (otherwise merchants are going to mandate a debt collection agency).¹⁰⁸ A special form is called *Payment partially after delivery*, where a consumer does not pay the overall amount of ordered goods at once, but partially with pre-defined amounts and within a certain time frame.¹⁰⁹

Cash on delivery

Ordered goods are delivered to a consumer, but are only handed over after full cash payment.¹¹⁰ This payment method strongly depends on regions and LSPs who offer the service of collecting money in combination with a delivery.¹¹¹

⁹⁹ [39], p.88.

¹⁰⁰ [29], p.35.

¹⁰¹ [29], p.35.

¹⁰² [29], p.35.

¹⁰³ [29], p.35.

¹⁰⁴ [29], p.37.

¹⁰⁵ [29], p.37.

¹⁰⁶ [29], p.39.

¹⁰⁷ [29], p.39.

¹⁰⁸ [29], p.39.

¹⁰⁹ [29], p.39.

¹¹⁰ [29], p.39.

¹¹¹ [29], p.39.

Other

Other online payment methods are, compared to the mentioned online payment methods, sparsely used, have a low overall volume, or are not authorized by law. One method, which has become more popular over the last few years, are *Cryptocurrencies* such as Bitcoin.¹¹² Another method is *Mobile carrier billing* (or *Direct carrier billing*), where the invoice amount is billed via direct carrier billing.¹¹³

¹¹²[39], p.90.

¹¹³[29], p.39.

E-commerce fraud

3.1 Definition of e-commerce fraud

Fraud (from Latin *fraus*: deceit, offence, injury¹) is defined in the Austrian Criminal Code (*Strafgesetzbuch*) as a proceeding including “*Vorsatz, durch das Verhalten des Getäuschten sich oder einen Dritten unrechtmäßig zu bereichern, jemanden durch Täuschung über Tatsachen zu einer Handlung, Duldung oder Unterlassung verleitet, die diesen oder einen anderen am Vermögen schädigt*”². (English translation: “[...] deceiving another about material facts causes the person to do, tolerate or omit an act which causes financial or other material loss to the other person or to a third person and who has the intention to gain an unlawful material benefit for himself, herself, or a third person [...]”³). This definition is restricted to financial losses, omitting non-financial losses, such as competitive advantage or reputation.⁴ A broader definition, covering tangible and intangible outcomes alike, is the “*act or course of deception, an intentional concealment, omission, or perversion of truth, to (1) gain unlawful or unfair advantage, (2) induce another to part with some valuable item or surrender a legal right, or (3) inflict injury in some manner*”⁵.

Different prefixes are used when naming fraud committed via the Internet: *Internet* fraud, *online* fraud, *digital* fraud, *net* fraud, *virtual* fraud, *cyber* fraud (or cyberfraud) and *e*-fraud (or electronic fraud).⁶ Albeit some of the terms are used more predominantly than others nowadays or are more common in specific domains (for example, *cyber* is predominantly used in the domain of security and crime), the prefixes can be used

¹[40].

²§ 146 StGB [41].

³[42], p.190.

⁴[43], pp.25–26.

⁵[44].

⁶[45], pp.14–15.

interchangeably.⁷ It has to be noted that while the prefix “e-” (or “electronic”) does not only comprise the Internet as medium of communication, but also other electronic means such as phone or fax, the definitions of e-fraud are usually addressing fraud committed via the Internet only.⁸

Using the definition of fraud as mentioned above, fraud committed via or facilitated by the Internet can therefore be defined as an “*act or course of deception, an intentional concealment, omission, or perversion of truth, to (1) gain unlawful or unfair advantage, (2) induce another to part with some valuable item or surrender a legal right, or (3) inflict injury in some manner, committed via the Internet*”.

Following this logic, *e-commerce fraud* can therefore be defined as an “*act or course of deception, an intentional concealment, omission, or perversion of truth, to (1) gain unlawful or unfair advantage, (2) induce another to part with some valuable item or surrender a legal right, or (3) inflict injury in some manner, by targeting e-commerce transactions*”.

E-commerce fraud is also known by other names. Some terms focus on the payment part or on a specific payment method: *Payment fraud, payment card fraud, online payment fraud, credit card fraud, debit card fraud, card-not-present fraud, carding, or behavioural fraud* (the illegitimate usage of a credit card or credit card data).^{9,10,11} Some of the aforementioned terms do not reveal where the fraud occurs (i.e. offline or online); they also fail to reveal that more than a fraudulent payment is necessary to commit e-commerce fraud. The term *transaction fraud* is, therefore, more comprehensive, as it covers the whole e-commerce transaction.¹² However, the word transaction is used in many different contexts and is not solely used in the context of e-commerce. Thus, the name *e-commerce fraud* is more self-explanatory and provides a more holistic view.

In a way, e-commerce fraud can be seen as the monetization of identity fraud and stolen payment information.¹³ Using stolen payment information (such as credit card data) to directly withdraw money is difficult, restricted (withdrawal limits), and also risky for fraudsters (as it bears the risk of exposing their location and true identities).¹⁴ Therefore, fraudsters commit e-commerce fraud, typically purchasing high-value products with the intention to resell them.^{15,16} To remain unknown and avoid prosecution, they use intermediaries to receive the fraudulently obtained goods.^{17,18} Upon reception, the goods

⁷[45], pp.14–15.

⁸[43], p.21.

⁹[46], pp.10–12.

¹⁰[47], pp.5–6.

¹¹[48], pp.603–604.

¹²[49], pp.362–364.

¹³[50], p.37.

¹⁴[51], p.1081.

¹⁵[8], p.29.

¹⁶[52], p.32.

¹⁷[51], p.1081.

¹⁸[52], p.32.

are usually sold via online marketplaces.^{19,20}

3.1.1 1st vs. 3rd party e-commerce fraud

It must be differentiated between *first party e-commerce fraud* and *third party e-commerce fraud*.

First party e-commerce fraud, also known as *friendly fraud*, is defined as “fraud committed by a genuine customer that does not involve the use of stolen identity or third party involvement”²¹, wherefore “the customer is the party who has acted dishonestly by violating the contract terms, in order to profit from their dishonesty”²².

Four forms of *first party e-commerce fraud* are distinguished: a) Chargeback, b) “Deshopping”, c) Bust out, and d) Misrepresentation of details.²³ In the case of a), a customer fraudulently reports a legitimate payment to obtain a refund by claiming not to have purchased the goods in dispute.²⁴ This can either be accidental (for example, if a family member is using a payment method for a purchase without the knowledge of the legitimate account holder) or intentional (which can be seen as a virtual form of shoplifting).^{25,26} Other ways are to claim a refund by stating to not have received the goods or services or only a part of them (despite having received the whole order), or to claim a refund by stating that the goods were returned and must have been lost in transit (despite not having sent them back).²⁷ In the case of b), customers order products with the intention to use them and return them after use to receive a refund.²⁸ For c), customers spend some time to appear trustworthy, often resulting in increased credit facilities, and then make purchases to the credit limit within a short period of time before disappearing to evade payment.²⁹ With regards to d), customers intentionally misrepresent their details to gain an advantage, for example, if they have already reached their credit limit with an account, they create another account and alter their details to appear as new customers.³⁰

It is often very difficult to tell whether such a claim by a customer is a fraud attempt or depicts the truth.^{31,32} Chargeback claims are very hard to detect as they often don’t follow a specific pattern, but can often be considered as “opportunity makes the thief”. To get a grip on “deshopping”, altering the return policies can reduce fraudulent behaviour.³³

¹⁹[8], p.29.

²⁰[53], p.8.

²¹[54], p.806.

²²[54], p.808.

²³[54], pp.809–812.

²⁴[54], p.811.

²⁵[54], p.811.

²⁶[55], p.30.

²⁷[54], p.811.

²⁸[54], p.809.

²⁹[54], pp.811–812.

³⁰[54], p.812.

³¹[55], p.30.

³²[56], pp.12–13.

³³[54], p.810.

Bust out has specific characteristics that can be detected, though it is often not possible to tell if purchases are done with the intention to commit fraud or not.³⁴ Misrepresentation of details can be prevented by using address verification systems and credit checks.³⁵

In contrast, *third party fraud* is committed by anonymous third party criminals that pretend to be legitimate customers.³⁶ They either steal the identity of a person, real or deceased, or “grow” an identity by counterfeiting documents.³⁷ Using this identity, they initiate an e-commerce transaction by placing an order, and either pay by using a payment method that is attributed to the impersonated person, or by using a payment method that allows the fraudster to receive an order before a payment must be made. To receive the ordered goods, they either use the vulnerabilities of delivery services (such as re-routing of a delivery; cf. 3.3.3 ‘Vulnerabilities of delivery services’), or use so-called mules (clueless people, recruited by criminals, who receive a delivery and re-ship it; cf. 7.1.1 ‘Reshipping-as-a-Service’). Another way to gain financial advantage by committing e-commerce fraud is the so-called triangulation scheme, where the fraudster purchases a good from a merchant, and directly sells it on another website, like an auction platform, where it is bought by a clueless buyer.³⁸ The fraudster instructs the merchant to send the order to the address of the buyer, whilst in return the buyer sends the payment to the fraudster.³⁹

3.2 Relevance and impact of e-commerce fraud

Figures about e-commerce fraud are scarce, and data is not reported in a unified way.⁴⁰ Reasons for that are different focuses (for example, the victim perspective, i.e. the merchant as a victim versus the consumer as a victim), and, as no uniform definition of e-commerce fraud exists, reported data deviates in terms of content. For example, most reports do not differentiate between 1st and 3rd party e-commerce fraud (which is often not even possible), or only focus on specific payment methods.^{41,42} Furthermore, a large part of e-commerce fraud is not reported by merchants, as they tend to tolerate and absorb parts of the losses.^{43,44} This is aggravated by the fact that fraud is often not discovered immediately, but after some time or not at all.⁴⁵

What all reports have in common is that they point out that e-commerce fraud has

³⁴[54], pp.811–812.

³⁵[54], p.812.

³⁶[57], pp.7–8.

³⁷[49], pp.364–366.

³⁸[56], p.13.

³⁹[56], p.13.

⁴⁰[58], p.6.

⁴¹[4], pp.12–14.

⁴²[58], pp.6–7.

⁴³[59].

⁴⁴[11], p.34.

⁴⁵[60], pp.259–260.

increased over the last few years, and is expected to increase further.^{46,47} The ever-growing volume of e-commerce transactions results in more cases of fraudulent transactions, as well as an increase in the ratio of targeted transactions.⁴⁸ As a result, the overall costs of fraud, i.e. the losses for merchants and the indispensable expenditures to fight fraud, are on the rise.^{49,50} Additionally, the increase is reinforced by measures against so-called “card-present” fraud (i.e. the fraudulent usage of physical credit and debit cards offline) which were established in the last few years, leading to a shift, and consequently, to an increase in card-not-present fraud.^{51,52}

In the following section, the impact of e-commerce fraud on consumers, merchants, and payment facilities is discussed.

3.2.1 Impact on consumers

Consumers are usually least affected by e-commerce fraud (at least from a financial point of view).⁵³ The combination of consumer protection legislation as well as consumer protection policies and insurance schemes of payment facilities allows consumers to dispute a payment easily.^{54,55} If a customer disputes the legitimacy of a payment and the claim is successful, it results in a so-called “chargeback”, i.e. the money is refunded.^{56,57}

A claim for a refund is investigated by the payment facilities and, subsequently, by the merchant. The burden of proof is the responsibility of the merchant; if the merchant can't prove the proper fulfilment of an order, the consumer receives a refund and the merchant has to bear the costs.^{58,59} Therefore, the losses for a consumer are usually manageable:

Time and effort

Consumers have to invest some time to dispute a fraudulent transaction, and, in some cases, file a complaint to the executive authorities.⁶⁰ This cost factor is in terms of time, as it can't be expressed in terms of money.

⁴⁶[4], pp.15–16.

⁴⁷[61], p.2.

⁴⁸[4], p.11.

⁴⁹[4], p.25.

⁵⁰[62], p.9.

⁵¹[52], p.32.

⁵²[11], p.34.

⁵³[63], p.6.

⁵⁴[64], p.1722.

⁵⁵[51], p.1088.

⁵⁶[65], p.4.

⁵⁷[63], p.6.

⁵⁸[51], p.1088.

⁵⁹[63], p.7.

⁶⁰[51], p.1088.

3.2.2 Impact on merchants

As mentioned above, in the case of disputed transactions, merchants are responsible to prove that the fulfilment of a transaction has been carried out properly and diligently.⁶¹ Evidence to prove that, for example, is the proof of delivery (i.e. the digital signature of a consumer to confirm the receipt of a delivery). In most cases, merchants don't have any or enough evidence to dispute the claim of a consumer.⁶² As a result, merchants are held responsible to cover all costs of a fraudulent transaction. The total costs are composed of several items:

Cost of lost goods

Merchants have to write off the value of the goods lost due to a fraudulent transaction.^{63,64}

Shipping expenses

Merchants make use of delivery services for shipping orders, and are, therefore, also responsible for their payment. Hence, in cases of chargebacks, merchants also have to bear the costs that have to be paid for the delivery.^{65,66} As time is of high relevance for fraudsters (the faster they receive the goods, the lower the likelihood that the fraud is detected prior to delivery), they usually request high-priority shipping; thus shipping costs in fraudulent transactions are often over-average.⁶⁷

Dispute fees

If a merchant does not have enough evidence to prove the proper fulfilment of a transaction, therefore being held responsible for the losses by the payment facilities, they are additionally charged with fees.^{68,69} On the one hand, these fees involve a fixed processing fee that has to be paid for each chargeback case.⁷⁰ On the other hand, depending on the chargeback rate of a merchant over a certain period of time, merchants can also face an additional surcharge.⁷¹

Additionally, if a merchant is not able to get a grip on fraudulent transactions that generate chargebacks, exceeding a certain threshold within a defined time frame, payment facilities will withdraw their service.⁷²

⁶¹[63], p.7.

⁶²[63], p.7.

⁶³[51], p.1088.

⁶⁴[65], p.4.

⁶⁵[51], p.1088.

⁶⁶[65], p.4.

⁶⁷[66].

⁶⁸[51], p.1088.

⁶⁹[65], p.4.

⁷⁰[67].

⁷¹[67].

⁷²[65], p.4.

Administrative costs

Every dispute requires a merchant to invest resources (like time and manpower) to investigate the matter, gather evidence to prove the proper fulfilment of an order, and communicate with the claiming customer and the payment facility.⁷³

3.2.3 Impact on payment facilities

In some cases, the payment facilities (e.g. banks, card issuers) cover the costs and refund the amount of dispute.⁷⁴ In any case, payment facilities have to bear the following costs:

Administrative costs

If a consumer claims a refund, the payment facilities start investigating the matter. These costs are charged to the merchant (at least to a certain extent) if the merchant is held responsible for the fraudulent transaction.⁷⁵

Reduced usage

If a legitimate account holder falls victim of a fraudulent use of a payment method, the loss of confidence can reduce the usage of the payment method or even a shift to an alternative payment method.⁷⁶ Thus, fraud can generate indirect costs by loss of customers.⁷⁷

Card re-issuance

If a card-based payment method was fraudulently used, a new credit or debit card must be re-issued and sent to the customer.^{78,79}

3.3 Anatomy of e-commerce fraud

As described in the previous chapter, an e-commerce transaction can be separated into three processes: *Agreement*, *Payment*, and *Delivery*. Following this separation, each process is analysed and the vulnerabilities regarding e-commerce fraud are highlighted.

3.3.1 Agreement

The agreement between a consumer and a merchant corresponds to the conclusion of a contract between them. Such a conclusion requires certain legal requirements (the

⁷³[64], p.1722.

⁷⁴[63], p.7.

⁷⁵[64], p.1722.

⁷⁶[57], p.5.

⁷⁷[49], p.364.

⁷⁸[68], p.15.

⁷⁹[51], p.1088.

legal aspects of the agreement and e-commerce fraud in general is analysed in detail in chapter 6 'Legal aspects and prosecution of e-commerce fraud'), i.e. that it is not based on deceit.^{80,81}

Important in the process of the agreement are, therefore, the concepts of *risk perception* and *trust*.⁸² Online transactions rely immensely on the trust between a consumer and a merchant.⁸³ Consumers have to trust the commitment of the merchant to handle the transaction confidently and reliably; and, vice versa, merchants have to trust consumers to be legitimate and to fulfil their part of the agreement by paying for the ordered goods and services.⁸⁴ The counterpart is the risk perception, which is the combination of “*uncertainty and the seriousness of the consequences of the purchase*”⁸⁵. The nature of the Internet increases the overall perceived risk in online transactions compared to physical buying processes.⁸⁶ Trust, however, has a positive impact on the perceived risk by reducing it.⁸⁷

In e-commerce transactions, merchants are not able to physically validate the identity of a consumer, and have to rely on the details stated by the consumer.⁸⁸ Paradoxically, merchants have to be moderate in their requests for information from their consumers, despite the fact that additional data could help merchants more precisely validate the legitimacy of a consumer.^{89,90} While fraudsters usually know basic details about a person to be able to fraudulently use their identity, they don't know more in-depth characteristics (for example, total number of credit cards of a consumer or the buying behaviour).⁹¹

E-commerce fraud is always based on deceit by a fraudster by committing *identity theft* and *identity fraud*.⁹² Identity theft is the unauthorized obtainment of an identity (“*unbefugte Sichverschaffen einer Identität*”⁹³). This comprises the acquisition of an identity by using the data of a real person to emulate their identity without their consent, as well as the creation of an identity with fictitious data.^{94,95} Identity fraud, however, is the unauthorized use of an identity (“*unbefugtes Agieren unter einer Identität*”⁹⁶). Therefore, identity theft is the prerequisite for identity fraud: An identity is prepared,

⁸⁰§ 861 ABGB [69].

⁸¹§ 870 ABGB [69].

⁸²[70], pp.331–332.

⁸³[54], p.805.

⁸⁴[70], pp.331–332.

⁸⁵[71], p.377.

⁸⁶[71], pp.377–379.

⁸⁷[72], p.113.

⁸⁸[73], p.937.

⁸⁹[49], pp.360–361.

⁹⁰[49], p.371.

⁹¹[49], pp.362–363.

⁹²[74], p.775.

⁹³[75], p.11.

⁹⁴[75], pp.10–11.

⁹⁵[76], p.556.

⁹⁶[75], p.9.

and identity fraud makes use of the prepared identity to commit fraud.^{97,98}

Measures to verify the identity of consumers are analysed in section 4.3 'Measures for identity verification'.

3.3.2 Payment

The timing and the order of the payment process in the e-commerce transaction affects who has to bear the risk in a common e-commerce transaction.⁹⁹ Three generic types of timing can be distinguished, as illustrated in figure 3.1: (1) Payment in advance, where the risk is with the buyer, (2) Payment afterwards, where the risk is with the seller, and (3) Simultaneous handover, where the risk is equally divided.¹⁰⁰

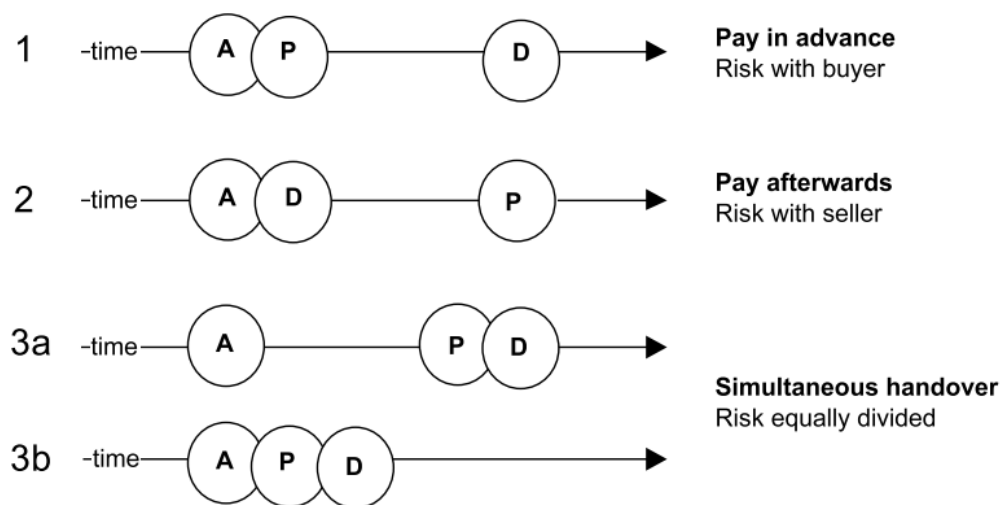


Figure 3.1: Timing and order of the e-commerce transaction processes¹⁰¹

Evaluation of online payment methods

In the following section, the online payment methods described in the previous chapter are evaluated concerning their risk regarding e-commerce fraud. It is summarized at the end with a table to provide an overview of the evaluation.

Of relevance for the evaluation of each payment method are the following questions:

- What is the timing of the payment and the delivery (i.e. payment before or after delivery)?

⁹⁷[75], pp.9–10.

⁹⁸[76], pp.554–555.

⁹⁹[39], p.26.

¹⁰⁰[25], pp.219–221.

¹⁰¹Reprinted from [25], p.221.

- Can it be fraudulently used by a third party?
- Can a consumer (first party) claim a refund, resulting in a chargeback?

Credit card: Online payment via credit card is integrated in the order process, and merchants receive the money (or at least a warrant to receive it soon after, as the transfer of money is not completed in real-time) before the consumer receives the delivery.

Due to the way credit cards are used to pay online and the wide dissemination and acceptance, it is the most common payment method used in fraudulent transactions.¹⁰² While it is a reasonably secure way to pay offline (the so-called “card-present” situation where a credit card can be swiped through a card reader; consumers have to sign a receipt; and merchants can check the card and compare the signatures on the receipt and the card, and obtain a proof of transaction in the form of a signed receipt), it poses a considerable risk in the online world, termed as “card-not-present”. In card-not-present transactions, it is not possible to prove the true identity of the card holder, meaning that there is no way to determine whether the card is being used by the legitimate card holder or by a third party.¹⁰³

In recent years, credit card companies tried to increase the security of online credit card payments by introducing security measures like “3D Secure” (chapter 4.4 ‘Security measures provided by payment methods’ is dedicated to this topic), which requires card holders to authorize transactions with a TAN or password.¹⁰⁴ Although these measures can reduce the potential of credit cards being used fraudulently, they are not used universally.¹⁰⁵ Therefore, it is still common to pay online using only the information that is printed on the credit card, which, consequently, allows credit cards to be used by third parties fraudulently.

In contrast to card-present situations, where the issuer is usually liable in the case of a fraudulent transaction, card-not-present transactions reverse the burden to the merchants.¹⁰⁶ Consumers are usually extensively protected and it’s easy for them to claim a refund for a transaction.¹⁰⁷

Debit card: The handling of debit cards for online payments is quite similar to that of credit cards, but consumer protection is usually not as strong and is contingent on the country and the policy of the issuer.^{108,109} For example, in the US, where debit cards are widely used, federal laws offer a staggered protection: If a refund is claimed within two days, the consumer is liable for up to 50\$, within 60 days for up to 500\$, and if not

¹⁰²[29], p.32.

¹⁰³[21], p.485.

¹⁰⁴[29], p.33.

¹⁰⁵[46], p.11.

¹⁰⁶[77], p.3.

¹⁰⁷[63], p.7.

¹⁰⁸[29], p.33.

¹⁰⁹[78].

reported within these 60 days for 100% of the transaction value.¹¹⁰ Nevertheless, some issuers offer protection that is equal to the protection of a credit card.¹¹¹

As a debit card is always directly linked to its respective bank account, and money is withdrawn immediately after a payment, it can also take several days until the money is refunded in the case of a chargeback.¹¹²

Pre-paid card: Pre-paid cards are quite similar to credit cards or debit cards with the difference that only the loaded amount of money can be spent.¹¹³ Consumer protection can be similar to that of credit cards/debit cards, or significantly less, depending on the country and the policy of the issuer.¹¹⁴

Prepayment: The consumer initiates the payment, and the fulfilment is usually on hold until the merchant receives the money and continues the process.¹¹⁵

An online prepayment via bank transfer has to be manually initiated and authorized by the account holder by signing it using some form of TAN. Once a merchant receives the money in its bank account, it can't be reversed by a consumer, therefore there is no chargeback risk for merchants.¹¹⁶ Due to the strict authentication of the legitimate owner, merchants can't be held accountable in the case of fraud.¹¹⁷

In the case of gift cards and vouchers, merchants have already received the money in the moment of purchase. With regards to pre-paid cards, merchants receive the money from the issuing authority of the pre-paid cards after they are used for payment.¹¹⁸ These cards and vouchers are non-personal, therefore they can be used by anyone.¹¹⁹

Electronic wallet: To use an e-wallet, access details (usually username and password) are necessary to authenticate oneself as the holder of an account and to complete payments.¹²⁰ Since anyone knowing the credentials of an account can access and use it, it is also prone to fraud. Not only is account takeover relevant, the creation of an account is usually very simple, and often no proof of identity is required (only an e-mail address). The chargeback risk of e-wallets is also related to the payment methods used in the background (e.g. a credit card or bank account).¹²¹

¹¹⁰[79].

¹¹¹[78].

¹¹²[78].

¹¹³[29], p.33.

¹¹⁴[79].

¹¹⁵[80], p.6.

¹¹⁶[29], p.35.

¹¹⁷[29], p.35.

¹¹⁸[39], p.88.

¹¹⁹[29], p.33.

¹²⁰[80], p.6.

¹²¹[29], p.35.

In addition, the usage of e-wallets is integrated seamlessly in the order process, and the merchants receives the payment (or at least a warrant that guarantees the payment to the merchant's account within a narrow time frame) ahead of the delivery.¹²²

E-wallet providers often offer protection for consumers (e.g. for transactions they did not conduct) and for merchants (if they can prove that their fulfilment was according to the guidelines).^{123,124}

Bank transfer: The online payment via bank transfer is seamlessly integrated in the order process: consumers have to authenticate themselves and authorize the payment, which is processed in real-time by the consumer's bank. The transfer of the money itself is not processed in real-time; however, merchants receive a warrant from the customer's bank that the payment will be credited to their account, resulting in the payment taking place prior to delivery.¹²⁵

The conditions are similar to those of prepayments via bank transfer, i.e. the strict authentication of the legitimate owner prohibits claims for refunds; therefore, merchants don't have to face chargebacks once they have received the money in their account.¹²⁶

Direct debit: Consumers give a mandate to merchants which allows them to initiate a payment and withdraw money from the consumer's bank account.¹²⁷ Such a mandate only states that the merchant has the consumer's authorization to withdraw money, it is not bound to a certain amount.¹²⁸ Therefore, to protect customers from unwarranted withdrawals, they can claim a refund on direct debit transactions, and subsequently, merchants can face chargebacks.¹²⁹ For example, the SEPA schema allows consumers to claim a refund within 8 weeks, and, if the transaction was initiated without a valid mandate, up to 13 months.¹³⁰

Direct debit mandates can be forged by third parties. Therefore, direct debit is prone to fraud, at least for a short time until an account holder notices illegitimate withdrawals.

Payment after delivery: Consumers receive the ordered goods or services before they have to make a payment via bank transfer.¹³¹ Therefore, there is no risk of a chargeback for merchants once they have received the payment of a consumer (cf. Prepayment and Bank transfer).¹³² However, merchants not only have to cover all costs in advance, but

¹²² [29], pp.33.

¹²³ [81].

¹²⁴ [82].

¹²⁵ [29], p.35.

¹²⁶ [29], p.35.

¹²⁷ [29], p.37.

¹²⁸ [29], p.37.

¹²⁹ [29], p.37.

¹³⁰ [29], p.37.

¹³¹ [29], p.38.

¹³² [29], p.38.

also have no guarantee that a consumer is willing or able to pay the invoice. This payment method can be taken advantage of by a third party as it does not require any form of authentication.

Cash on delivery: Before the delivery is handed over to the consumer, the order must be paid in cash.¹³³ In theory, this payment method could be used by a third party, albeit it would be contradicting the idea of fraud.

Since a consumer receives the delivery only upon full payment (and vice versa, the payment is only done in expectation of receiving the delivery), a consumer can't claim a refund. Moreover, there is no payment facility involved to handle a chargeback.¹³⁴

Summarization: Table 3.1 provides an overview of the evaluation of online payment methods regarding their potential to be used in e-commerce fraud.

In the column "Security", the rating ranges from *none* (no security at all), *low* (payment details are necessary), *medium* (static username and password) to *high* (generated, one-time code). Bank transfers are considered to have a high security rating, as it requires some form of TAN to authorize a payment. In the case of credit cards, debit cards, and pre-paid cards, the security rating is either high or medium (when 3D Secure is used, either with a password or a TAN) or low (if only the card details are necessary to make a payment). In the case of prepayment, it must be distinguished between prepayment via bank transfer (high security) and payment with vouchers, gift cards, and pre-paid cards (no security).

The rating for column "Payment before delivery" is either *yes*, if a merchant receives the payment (or at least a warrant that the payment will be received shortly) before the order is delivered to the consumer, or *no*, if a consumer receives the delivery and pays afterwards. Only payment method *Payment after delivery* allows consumers to pay after receiving an order.

Column "Risk of third party usage" rates the risk if a payment method can be used (not only, but also fraudulently) by a third party. The rating ranges from *low* (risk-free or nearly risk-free), *medium* (moderate risk of usage by third parties) to *high* (considerable risk of third party usage). Again, it must be distinguished between prepayment via bank transfer (low risk of usage by third parties) and gift cards, vouchers, and pre-paid cards (high risk of usage by third parties as these are non-personal means of payment). The risk is also high for credit cards, debit cards and pre-paid cards if 3D Secure is not used; in contrast, if 3D Secure is used, the risk of usage by third parties is reduced to the rating *low* (as not only the card details would be necessary, but also the 3D Secure code, i.e. a TAN or password).

The risk of a chargeback for a merchant is rated in the second to last column. The rating ranges from *none* (no chargeback risk), *low* (hardly any chargeback risk), *medium*

¹³³[29], p.39.

¹³⁴[80], p.6.

Payment method	Security	Payment before delivery	Risk of third party usage	Risk of chargeback	Overall risk rating
Credit card	low-high	yes	high/low	high	high-low
Debit card	low-high	yes	high/low	high	high-low
Pre-paid card (credit/debit)	low-high	yes	high/low	high	high-low
Prepayment (bank transfer)	high	yes	low	low	low
Prepayment (voucher, gift card, pre-paid card)	none	yes	high	low	low
Electronic wallet	medium	yes	medium	medium	medium
Bank transfer	high	yes	low	low	low
Direct debit	low	yes	medium	medium	medium
Payment after delivery	none	no	high	none	high
Cash on delivery	none	yes	low	none	low

Table 3.1: Evaluation of online payment methods

(moderate chargeback risk) to *high* (high chargeback risk). The chargeback risk is the highest with credit cards, debit cards, and pre-paid cards.

Overall, the risk for merchants is the lowest with *Prepayments*, *Bank transfers* and *Cash on delivery*. *Payment after delivery*, and payments via *Credit card*, *Debit card* and *Pre-paid cards*, if 3D Secure is not used, pose the highest risk for merchants.

As it seems obvious which payment methods pose the highest risk for merchants to fall for a fraudulent transaction, the following question arises: what keeps merchants from avoiding specific payment methods. This issue is further analysed in section 4.5 'Restriction of payment methods'.

3.3.3 Delivery

Delivery is not only the last process in an e-commerce transaction, but also the last obstacle for fraudsters to successfully complete their fraud attempt.

There are various ways in which fraudsters can successfully receive the ordered goods. Some of them require preparation and certain knowledge (such as the route of a delivery agent, or if a home-owner is at home during the day or not), while others require the involvement of additional participants. In addition, vulnerabilities exist in the delivery of goods, depending on the way an order is delivered. While cases of fraud can't be revealed based on a customer's selected method of delivery, since they are also used by ordinary customers, certain methods of delivery can be exploited by fraudsters.

Vulnerabilities of delivery services

In the following section, the vulnerabilities of various delivery methods are highlighted.

Unattended delivery: This comprises all delivery types where the delivery is dropped-off at a certain place. It can be differentiated between unsecured and secured delivery.¹³⁵

Unsecured delivery: In this case, the delivery is placed at the doorstep or somewhere outside the house.^{136,137} Fraudsters can wait until the agent deposits the delivery and then pick up the order. Due to the lack of a POD (proof of delivery), it is not possible to uncover what happened to the delivery.¹³⁸

Secured delivery: The delivery is dropped-off at a certain, secured location.¹³⁹ Some of these solutions are unattractive to fraudsters, as they prevent access to the goods (for example, *Home Access Systems*, where delivery agents have access to a secure place outside or in the house, such as a shed or the garage), require personal interaction, or even an ID check when picking up a delivery (for example, neighbours, post offices, local shops or gas stations).^{140,141} On the contrary, reception boxes (also termed locker points or packet stations) are secured locations as well, but they are unattended.¹⁴² Picking up a delivery requires no personal interaction and can be done anonymously.¹⁴³ Usually, only a code is needed to open the box, which is sent by the delivery company to the recipient.¹⁴⁴

¹³⁵[83], p.31.

¹³⁶[83], p.31.

¹³⁷[84], p.24.

¹³⁸[83], p.32.

¹³⁹[85], pp.182–184.

¹⁴⁰[86], pp.25–28.

¹⁴¹[85], pp.182–184.

¹⁴²[8], p.43.

¹⁴³[87].

¹⁴⁴[88], pp.640–641.

Delivery interception: Another way for fraudsters to receive the fraudulently ordered goods is to intercept the delivery agent at the delivery address by impersonating either the recipient or a member of the household.¹⁴⁵ While the first case might only work under special circumstances (for example, a new delivery agent who does not know the recipients on the delivery route), the latter case benefits from the fact that a delivery is usually handed over to anyone from the same household.¹⁴⁶ Moreover, it is uncommon that the ID of a recipient is checked by a delivery agent, as this is usually an additional, fee-based service.^{147,148}

Delivery forwarding: Fraudsters make use of delivery forwarding by appearing to be in the same country as the merchant to avoid raising the merchant's suspicion, or to cover their identities and real addresses.^{149,150} They either make use of freight forwarding companies or a reshipping scheme.^{151,152}

Freight forwarding: A freight forwarding company handles the import and export of goods between international destinations.¹⁵³ Fraudsters use it to receive the fraudulently ordered goods in countries abroad that are often perceived by merchants as high-risk locations.¹⁵⁴ They use local addresses provided by the freight forwarding companies, allowing them to appear to be in the same country as the merchant, avoiding a declination of the transaction because of their real location.¹⁵⁵

Reshipping: In this case, fraudsters make use of unsuspecting people (called *mules*) who receive, repack and reship packages, usually to international destinations.^{156,157} The advantages for fraudsters by using mules to receive their orders is that they can receive their packages in international, often high-risk countries, even though a merchant would not ship to these countries.¹⁵⁸ Moreover, it allows them to not only camouflage their true identities; the legitimate shipping addresses of mules do not raise the merchant's suspicion.^{159,160} It is common for fraudsters to not operate their own reshipping scheme,

¹⁴⁵ [86], p.11.

¹⁴⁶ [86], p.34.

¹⁴⁷ [89].

¹⁴⁸ [90].

¹⁴⁹ [30], pp.158–159.

¹⁵⁰ [91].

¹⁵¹ [92].

¹⁵² [52], p.32.

¹⁵³ [93].

¹⁵⁴ [91].

¹⁵⁵ [30], pp.158–161.

¹⁵⁶ [51], p.1082.

¹⁵⁷ [94], p.19.

¹⁵⁸ [51], p.1082.

¹⁵⁹ [51], p.1082.

¹⁶⁰ [94], p.19.

but rent mules from so-called *operators* specialized in operating mule networks (termed *Reshipping-as-a-Service*, cf. 7.1.1 'Reshipping-as-a-Service').¹⁶¹

Delivery rerouting: There are two different approaches: Either the merchant is contacted after the payment process and asked to send the delivery to another address, or the delivery service is contacted and a rerouting is requested after the goods are shipped by the merchant.^{162,163} In the latter case, the merchants are often not aware of the change of the delivery address.¹⁶⁴ In both cases, however, the re-routing is requested after the order has been reviewed and accepted; thus, it is used by fraudsters to avoid raising suspicion (for example, by using the address of the legitimate account holder of a payment method).¹⁶⁵

Evaluation of the risk potential of delivery vulnerabilities

The evaluation regarding the risk potential of vulnerabilities of delivery services is summarized in table 3.2.

The table consists of the following columns:

- Suspicious characteristics (yes/no): It is evaluated whether this vulnerability has certain characteristics that can help a merchant to identify a fraud attempt.
- Anonymous (yes/no): As fraudsters want to keep their real identity hidden, it is rated if this vulnerability allows them to stay anonymous.
- POD (yes/no): This column contains the evaluation whether a POD is existent or not.
- Circumvent destination limitation (yes/no): As some merchants limit the delivery to countries that are perceived as high-risk locations, it is rated if the vulnerability can be used to circumvent the limitation.
- Complexity (low/medium/high): The complexity to exploit this vulnerability is evaluated. It comprises necessary preparations, certain knowledge, and the effort to accomplish it.
- Overall risk potential (low/medium/high): This column contains the overall risk potential, derived from the ratings of the other columns.

An *Unattended delivery* allows a fraudster to stay anonymous, and it does not raise suspicion, as these ways of deliveries don't have any certain characteristics that could

¹⁶¹[51], p.1082.

¹⁶²[95], p.236.

¹⁶³[96].

¹⁶⁴[95], p.236.

¹⁶⁵[95], p.236.

Delivery vulnerability		Suspicious characteristics	Anonymous	POD	Circumvent destination limitation	Complexity	Overall risk potential
Unattended delivery	Unsecured	no	yes	no	no	medium	high
	Secured	no	yes	no	no	low	high
Delivery interception		no	no	yes	no	medium	medium
Delivery forwarding	Freight forwarding	yes	no	yes	yes	low	medium
	Reshipping	no	no	yes	yes	low	high
Delivery rerouting		no	no	yes	no	low	medium

Table 3.2: Evaluation of the risk potential of delivery vulnerabilities

indicate fraud. It can't be used to circumvent destination limitations, as the goods are delivered to the address given by the merchant or a location near that address. A fraudster has to put some effort in *Unattended, unsecured deliveries*, as it is necessary to know whether someone is home during the estimated time of the delivery. Moreover, a fraudster must make sure that an order is left unsecured at the address, otherwise (for example, if the delivery is handed over to a neighbour) there is no way of receiving it. Both cases of *Unattended delivery* lack a POD. Overall, the potential for fraudulent usage is high.

A *Delivery interception* is similar to *Unattended, unsecured deliveries*, with the difference that a fraudster actively tries to receive the delivery. Some preparations are required: A fraudster must be present to intercept the delivery agent; therefore, it is necessary to know the estimated delivery time. To not raise suspicion, they also have to impersonate either the recipient of the delivery or a member of the household. A POD is signed by the fraudster, but it is worthless due to the impersonation. This way of delivery does not allow a fraudster to stay anonymous, but the real identity is hidden by the impersonation. The overall potential for this exploitation of vulnerability is medium, as the success depends on the trusting of the delivery agent.

Delivery forwarding allows fraudsters to circumvent destination limitations by a merchant. In both cases, a POD is signed, and the necessary effort is low (it is assumed that fraudsters don't recruit their own mules, as it is common that they use the mule network of other criminals). Additionally, fraudsters do not remain completely anonymous, as they have to receive the delivery. While *Reshipping* can't be detected, since the recipients are legitimate consumers, *Freight forwarding* has certain characteristics, such as the addresses of the freight forwarding companies or the address format that can help merchants to identify it. Therefore, the overall risk potential rating for *Freight forwarding* is medium, whereas the risk potential of *Reshipping* is high.

Delivery rerouting is easy to conduct and requires little effort by the fraudster. Since the rerouting is requested usually after fraud checks are conducted by merchants, it does not raise suspicion. Using this method of delivery, the fraudster does not stay anonymous as the parcel is eventually handed over and a POD is signed. The overall risk potential is medium, as it depends on the good will and trust of a merchant or delivery company; additionally, the option for a rerouting is often prohibited a priori.

Fraudsters can also combine these methods of delivery. This allows them to sophisticatedly exploit the vulnerabilities of multiple delivery methods, ensures better coverage of the fraudster's tracks, conceals their true identity, and raises less suspicion from merchants.

3.4 Indicators of e-commerce fraud

In general, people who commit fraud do not differ from ordinary people.¹⁶⁶ Demographic or psychological characteristics can't be used to tell whether someone is more likely to commit fraud or not.¹⁶⁷ However, from a demographic perspective, fraudsters are from all social classes, are of all ages (from teenagers to seniors), and tend to be male.^{168,169} From a psychological perspective, some personality traits are risk factors for fraud: Antisocial personality disorder, narcissism, and psychopathy.¹⁷⁰ Fraudsters are more likely to be greedy and dishonest, but this applies to many ordinary people as well (who are law abiding and don't commit fraud).¹⁷¹

Due to the reason that demographic information and personality traits can't reveal fraudsters, their virtual appearance and behaviour can be used to derive indicators for e-commerce fraud. The following characteristics of e-commerce fraud are closely related to the indicators and can help to explain them:

- Fraudsters have no intention to pay with their own money. They either use the payment information of someone else, or a payment method where they don't have

¹⁶⁶[97], p.33.

¹⁶⁷[97], p.33.

¹⁶⁸[49], p.366.

¹⁶⁹[98], pp.1–2.

¹⁷⁰[99], pp.224–228.

¹⁷¹[99], p.224.

to pay before receiving the order.

- Time is of the essence. The more time goes by, the higher the risk that an act of fraud is revealed or fails (for example, if a stolen credit card has been reported and is invalid).
- They want to keep their real identity secret, and therefore try to cover their tracks.
- E-commerce fraud is often a cross-border crime.

The indicators for e-commerce fraud, categorized in the processes of an e-commerce transaction, are explained in the following section.

3.4.1 Agreement

In the case of e-commerce fraud, order characteristics differ from average orders, such as the total price or the quantity of an item. Additionally, fraudsters try to emulate regular consumers, which also allows to derive indicators of fraud:

Larger-than-average orders

Fraudsters don't intend to pay with their own money, and stolen payment details have a limited life span. Therefore, they often place larger-than-average orders to maximize their profit.^{172,173}

Larger-than-average quantities of an item

To place large orders, fraudsters often order several items of the same kind (which is unusual for ordinary customers).^{174,175}

Expensive items

In general, fraudsters are aiming at expensive goods - the higher the value, the higher the resell price.^{176,177}

First-time buyers exceeding a certain fraud detection minimum

First-time buyers should not be necessarily put under general suspicion, because every regular customer was once a first buyer.¹⁷⁸ Nevertheless, orders of first-time buyers that

¹⁷²[98], p.4.

¹⁷³[100].

¹⁷⁴[98], p.4.

¹⁷⁵[100].

¹⁷⁶[98], pp.3-4.

¹⁷⁷[100].

¹⁷⁸[66].

exceed a certain threshold (such as the average order of an ordinary first-buyer) can be a warning sign.¹⁷⁹

Orders at unusual times of day

Ordinary customers shop at ordinary times of day. Fraudsters, however, tend to either intentionally place orders at unusual times (for example, at night), where they perceive the risk of detection to be lower, or because they reside in a different time zone.¹⁸⁰

Inconsistencies

Mismatches in the order details can indicate fraud.¹⁸¹ For example, while it is not uncommon that the billing and shipping addresses are different (for example, in case of a gift), other details can reveal a fraud attempt.¹⁸² Fraudsters are likely to use the billing details from the legitimate account holder, but a different phone number. Therefore, if the area code (in case of a land-line) or the country code do not match the billing address, it can indicate a potential case of fraud.¹⁸³

3.4.2 Payment

One transaction is not suspicious, even multiple transactions do not have to arouse distrust. But in combination with other factors, such as the number of related accounts or the shipping address, indicators for fraud can be determined. The IP address can be helpful in these cases to determine if multiple accounts were created or multiple transactions were placed from the same Internet connection (assumed that a fraudster is not using a service to cover the real IP address). Common combinations are listed below:

Multiple transactions with the same method of payment in a short period of time

Either fraudsters try to test a method of payment in a real-time processing system (starting with low-value transactions to not attract the attention of a merchant and test if the method of payment is working), or they max out the credit limit and place as many orders as fast as possible before the fraudulent use is detected.^{184,185}

¹⁷⁹[101].

¹⁸⁰[98], p.3.

¹⁸¹[102], p.5.

¹⁸²[94], p.52.

¹⁸³[98], p.4.

¹⁸⁴[100].

¹⁸⁵[94], p.53.

Multiple transactions with the same method of payment, but shipping to multiple addresses

The reasons for this can be either to lay low and not attract the attention of a merchant, or to distribute the risk regarding the delivery of the orders.^{186,187} It can also be an indicator for a more sophisticated fraud scheme, namely the triangulation scheme as described before.

Multiple transactions with different accounts, but shipping to a single address

This can be a scheme by fraudsters to not attract the attention of a merchant by placing average orders using multiple accounts to mimic multiple consumers.^{188,189}

Multiple transactions with different methods of payment, but shipping to a single address

In this case, a fraudster is likely to be in possession of multiple methods of payment, using them to pay for multiple orders.^{190,191}

Multiple declined transactions

When fraudsters try to use a method of payment, it can happen that the purchase is declined by the PSP.¹⁹² If a fraudster tries again to place a transaction, for example with a lower amount to find out if the card is still valid or the credit limit has been reached, it can be an indicator for fraud.¹⁹³ It is all the more suspicious if this happens with multiple methods of payment for one single account or IP address.

3.4.3 Delivery

Regarding the delivery, the recipient and country of destination as well as delivery options can be indicators of e-commerce fraud:

Unreasonable shipment fees

As fraudsters don't intend to spend their own money, they also don't care about shipment fees. Therefore, shipment fees that are unreasonable (for example, if the shipment fees

¹⁸⁶[100].

¹⁸⁷[94], p.53.

¹⁸⁸[66].

¹⁸⁹[94], p.53.

¹⁹⁰[66].

¹⁹¹[94], p.53.

¹⁹²[101].

¹⁹³[66].

are exceeding the value of the ordered goods) can indicate fraud.^{194,195}

Express shipping

For a fraudster, time is of the essence, money is not. Therefore, they want the ordered goods as fast as possible before the fraud is revealed, often choosing an express shipment method.^{196,197}

International shipping

While not all international orders are suspicious, there are countries known to have a higher potential for fraudulent transactions. As mentioned previously, fraudsters don't worry about high international shipping fees.^{198,199}

Drop box addresses

Drop box addresses allow deliveries to be retrieved without proof of identity and signing a receipt, which is convenient for fraudsters.^{200,201}

Delivery forwarding

Some fraudsters use freight forwarders to not only cover their tracks, but to simulate being in the same country as the merchant (to avoid attracting attention due to a cross-border order).²⁰² Additionally, freight forwarders accept the delivery and sign it; therefore making a signature confirmation useless.²⁰³

¹⁹⁴[66].

¹⁹⁵[103].

¹⁹⁶[98], p.3.

¹⁹⁷[100].

¹⁹⁸[98], p.3.

¹⁹⁹[100].

²⁰⁰[98], p.3.

²⁰¹[101].

²⁰²[104].

²⁰³[104].

Preventing e-commerce fraud

4.1 General

Fraud prevention comprises measures to disable the occurrence of fraud before it occurs.^{1,2} Included are the means for each process of an e-commerce transaction to prevent fraud: Verification of the identity and data provided by a consumer in the agreement process, security measures and restriction of payment methods in the payment process, as well as actions to be taken to avoid delivery vulnerabilities in the delivery process. As fraud prevention is concerned with creating a setting to avoid fraud, it can not help to distinguish whether an occurring transaction is fraudulent or not.³ This requires fraud detection measures to analyse each transaction, therefore the subsequent chapter is dedicated to them.

4.2 Collection and analysis of fraudulent transactions and attempts

Collecting the data from fraudulent transactions and attempts allows merchants to learn from the past to brace themselves for the future.⁴ All key elements related to a case of fraud should be gathered.⁵ This comprises all information related to a customer, such as the name, mail address, phone number, billing and shipping addresses; as well as information regarding the payment method, such as the credit card number; and technical information such as the IP address.⁶

¹[105], p.236.

²[106], p.235.

³[107], p.315.

⁴[108].

⁵[94], p.84.

⁶[94], p.84.

By analysing the collected data, merchants can derive three advantages:

Firstly, it can help merchants to identify the reasons why fraudsters are targeting their system.⁷ This allows merchants to take countermeasures and reduce the overall vulnerability to e-commerce fraud.⁸

Secondly, the derivations can be used to create blacklists.⁹ Based on the collected data, these lists contain key elements that help to identify fraudulent transactions in the case of the same information being used in subsequent transactions, namely the IP address, the shipping address or the contact details.¹⁰ Such lists can be especially helpful to prevent repeated attempts by the same fraudster.¹¹

Thirdly, it allows merchants to derive patterns by detecting abnormalities in the data.¹² These patterns can reveal a higher risk depending on various factors, such as the time of day, geographical information, the payment method, delivery options, or certain specifications in the customer data.¹³ This enables merchants to define specific rules for e-commerce transactions to either flag for further review or even reject an order with fraudulent potential.¹⁴

4.3 Measures for identity verification

The verification of the identity of a consumer is one of the top issues merchants are faced with.¹⁵ Due to the absence of physical interactions, e-commerce transactions are prone to fraud attempts.¹⁶ Even by using different technologies and systems, it is almost impossible to fully verify the identity of a consumer.¹⁷ Another issue regarding identity is that it is based on documents (for example, passport or driver license), which can also be forged or illicitly obtained.¹⁸

Expectations from consumers also play an important role; therefore, measures for identity verification must be moderate.¹⁹ While it might be acceptable to undergo a thorough identity assessment in some cases, such as applying for financial services, this would not be the case for an e-commerce transaction.²⁰ Important in this context are also the privacy concerns of consumers.²¹ Even though it would be useful to gather as much

⁷[109].

⁸[109].

⁹[109].

¹⁰[63], p.9.

¹¹[30], p.200.

¹²[108].

¹³[108].

¹⁴[30], pp.203–207.

¹⁵[62], pp.15–16.

¹⁶[54], p.805.

¹⁷[110], p.2.

¹⁸[111], p.43.

¹⁹[49], p.360.

²⁰[49], pp.360–361.

²¹[49], p.371.

information about a consumer as possible, seeing as fraudsters are usually unable to provide more than the basic details required to commit fraud, this would raise privacy issues for customers.²²

Moreover, there is tension between measures to prevent fraud and user experience.²³ Consumers want fast and frictionless processes.^{24,25} Delays and above-average effort can result in unsatisfied consumers and ultimately in transaction and consumer loss.

Since returning consumers already have a purchase history, which allows merchants to better estimate the trade-off between risk and trust, the measures for identity verification discussed in the following section are focused on measurements for first-time consumers. The main issue with returning customers is authentication, i.e. ensuring that a transaction is performed by the legitimate account holder.²⁶

In the following section, measures for identity verification are explained.

4.3.1 Data verification

Data verification can be either done manually or automatically using third-party service providers.

The manual verification of the identity of a consumer can comprise of, among other ways, simply checking the address using online maps or phone directories, calling the consumer to verify the submitted data, contacting the issuer of the used method of payment to verify the billing address, or the usage of reverse lookup checks.²⁷ In the latter case, the information submitted by the consumer is cross-checked, i.e. parts of the data are entered into a lookup service and the result can be compared to the submitted information.²⁸ For example, entering the phone number in a lookup service returns the name and address of the associated person.²⁹ Manual verification is not only costly and time-consuming, but it can also delay a transaction and does not guarantee reliable results.^{30,31}

Service providers offering automated data verification maintain enormous amounts of customer records aggregated from data that stems from various sources, such as credit bureaus, governmental agencies, telecom companies, and public records.³² The information submitted by a consumer is matched against these customer records and discrepancies are identified.³³ This allows, for example, the usage of deceased identities to be detected,

²²[49], p.360.

²³[112].

²⁴[112].

²⁵[6].

²⁶[68], p.10.

²⁷[113].

²⁸[114].

²⁹[114].

³⁰[65], p.2.

³¹[73], p.940.

³²[115].

³³[116].

or to make sure that the entered data (such as the name, e-mail address, billing address and phone number) belongs to only one person and is used in other sources as well.³⁴

4.3.2 ID check

To verify the identity of an Internet user, the check of identity documents can be done both online and offline.

Online ID check

The online check of identity documents can be done in two ways: either by validating digital copies (i.e. scans or photographs) of identity documents, or via video chat.

Digital copies of identity documents are submitted to and checked by specialized service providers.³⁵ Key information contained in the submitted documents is extracted and validated automatically.³⁶ Additionally, the submitted identity documents are analysed for abnormalities that can indicate a forgery or alteration of the document.³⁷

The verification via video chat is done using a live video connection.³⁸ An agent of the company that provides that service verifies the identity document presented by the customer via web cam.³⁹ Moreover, the agent compares the photo of the presented identity document and the appearance of the customer and checks if they match.⁴⁰

Offline ID check

Verifying the identity of a consumer offline is typically carried out by a delivery company and can be offered as either a standalone service or in combination with a delivery.⁴¹ In the first case, a consumer has to visit a branch office to verify the identity by presenting adequate documents, or a delivery agent verifies the identity at the doorstep of the consumer.⁴² In the latter case, a delivery is delivered to a consumer, and the delivery agent checks the identity of the addressee before handing over the package.^{43,44}

4.3.3 Trusted virtual identity

To establish a trusted virtual identity, it is necessary for users to prove their identity to a provider that offers that service.⁴⁵ After a successful identity check, the trusted virtual

³⁴[117].

³⁵[118].

³⁶[119].

³⁷[120].

³⁸[121].

³⁹[122].

⁴⁰[122].

⁴¹[123].

⁴²[123].

⁴³[89].

⁴⁴[90].

⁴⁵[124].

identities can be used to authenticate themselves on other websites.⁴⁶ The authentication is secured, either with multi-factor authentication or a smart card.^{47,48}

Although this measure to ensure someone's identity is quite effective, these services are not wide-spread in the area of e-commerce and are mainly offered to citizens to get access to governmental services.^{49,50}

In summary, all measures to verify the identity of a consumer entail costs (as all of them require the utilization of a specialized service provider). Some of them have the potential to prevent the usage of fraudulent identities; however, most of them are not applicable for e-commerce transactions. The demand to receive an identity document from a consumer or to let a third-party service verify their identity to fulfil an order will most likely deter customers. In addition, it increases the effort of a consumer and delays the e-commerce transaction. A trusted virtual identity requires that consumers have already carried out the process or are willing to verify their identity with the specialized service provider. While it could be integrated effortlessly into an e-commerce transaction, the low-spread in e-commerce prevents a large-scale usage.

However, the delivery combined with an ID check can be a practical solution for first-time consumers, as it does not delay the fulfilment of the transaction and requires only minimal extra effort for consumers.

Automated data verification has no impact on the customer experience, as it does not generate additional effort for a consumer and is done in real-time; therefore, the transaction is not delayed. While it does not guarantee the complete verification of the identity of consumers, and is therefore not a suitable single solution to preventing fraud, it can provide an additional layer of security.

4.4 Security measures provided by payment methods

Recalling the evaluation of payment methods from the previous chapter, one of the evaluated factors was the security of the payment methods. Electronic wallets are secured with a password. Bank transfers (real-time and prepayments) are secured with a password as well, but TANs are additionally used to authorize a payment. Vouchers and gift cards don't provide any security (as they are not bound to a certain account holder); however, merchants have already received the money in advance and don't have to fear the risk of chargebacks. Cash on delivery does not provide any security measures, but it is secured by its nature, as the delivery is only handed over after payment is complete.

⁴⁶[124].

⁴⁷[125].

⁴⁸[126].

⁴⁹[127].

⁵⁰[128].

Direct debit payments are secured by a mandate that authorizes a merchant to withdraw money from a bank account. Such a mandate can be forged by a fraudster, allowing them to fraudulently use this payment method. Direct debit, however, does not pose a huge threat to merchants as it is usually used for low-value or recurring transactions, such as subscriptions, and its overall usage is not wide-spread.⁵¹

Payment after delivery poses a high threat to merchants, as it does not provide any security. If a customer does not pay the invoice, merchants can mandate a debt collection agency to collect the outstanding balance.⁵² An effective remedy against this risk is the usage of a specialized third-party payment provider.⁵³ These providers take over the process of handling the invoice.⁵⁴ Moreover, they guarantee the payment for the merchant, even in the case of a consumer not paying the invoice.^{55,56} Therefore, it also reduces the risk for merchants in the case of fraudulent transactions.

The risk of fraudulent payments with credit cards, debit cards, and pre-paid cards depends on the security measures in place. A main step towards more security when paying with cards was the invention of *Card Security Codes*.⁵⁷ Depending on the card issuer, it is a three- or four-digit value, usually printed on the back of a card.⁵⁸ It was invented to validate that the card account is legitimate and that the consumer using the card is in its physical possession.⁵⁹ The functional principle is, according to the PCI DSS⁶⁰, that merchants are not allowed to store credit card security codes, which ensures that the legitimate account holder must have been in physical possession of the card at least once.^{61,62} It is estimated that the card security codes reduced card-not-present fraud by up to 70% after their invention.⁶³

Card security codes were not sufficient to stop the fraudulent use of cards in online transactions, as cards could still be used by anyone in possession of the card details and the card security code (for example, in the case of stolen credit cards or phishing attacks).⁶⁴ Therefore, a technology termed *3D Secure* was invented. The name comes from the three domains (hence 3D) that are involved in the payment process: (1) The acquirer domain, i.e. the relation between merchant and acquirer, (2) the issuer domain,

⁵¹[39], p.88.

⁵²[29], p.38.

⁵³[29], p.38.

⁵⁴[29], p.38.

⁵⁵[129].

⁵⁶[130].

⁵⁷[30], pp.137–138.

⁵⁸[30], p.137.

⁵⁹[30], pp.137–141.

⁶⁰“*The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards designed to ensure that ALL companies that accept, process, store or transmit credit card information maintain a secure environment.*” [131].

⁶¹[132].

⁶²[133], p.9.

⁶³[134], p.9.

⁶⁴[73], p.940.

i.e. the relation between card holder and issuer, and (3) the interoperability domain, i.e. the relation between acquirer and issuer.⁶⁵ It is based on an authentication model that requires account holders to verify their identity when paying online, either by entering a password or a TAN to authorize the payment.⁶⁶ It has not only proven to be able to stop fraudulent card-not-present transactions, but has also lead to a partial liability shift with an increased protection from fraud for merchants.⁶⁷ 3D secure is an excellent deterrent, but it is still not used worldwide, thus not all online transactions are protected with it.⁶⁸

Important in this regard is the endeavour of merchants to focus on customer satisfaction. Customers want a simple, fast and frictionless shopping experience. Additional security measures are likely to be disliked by them, which can potentially reduce customer satisfaction, and ultimately result in the loss of customers.⁶⁹ Therefore, merchants are often willing to absorb and tolerate the losses, hence neglecting additional security measures.⁷⁰

4.5 Restriction of payment methods

As evaluated in the previous chapter (cf. 3.3.2 'Evaluation of online payment methods'), some payment methods depict a higher fraud risk than others for merchants. Therefore, it seems to be an obvious solution for merchants to simply avoid high-risk payment methods by not offering them to their consumers.

However, important for the selection of payment methods are regional support, consumer preference, customer base, and return on investment.⁷¹ Since two of these factors are directly related to consumers, ignoring them for the sake of fraud reduction can have negative effects. Not providing payment methods that are preferred by consumers can result in customers switching to competitors, cancelled transactions, and, consequently, in turnover loss.^{72,73}

Instead of generally restricting certain payment methods, a more effective solution would be to establish a consumer-specific risk management.⁷⁴ Considering the expected potential, value and risk of a consumer, as well as the risks of payment methods allows merchants to create a customer-specific risk-turnover rating per payment method.⁷⁵ Based on the trade-off between expected risk and expected turnover, a certain payment method can

⁶⁵[26], p.54.

⁶⁶[29], p.33.

⁶⁷[30], pp.146–151.

⁶⁸[46], p.11.

⁶⁹[11], p.34.

⁷⁰[11], p.34.

⁷¹[30], pp.4–6.

⁷²[135], p.69.

⁷³[136], pp.39–60.

⁷⁴[135], pp.68–69.

⁷⁵[135], pp.70–75.

either be offered to a consumer or be restricted.⁷⁶ This creates stricter standards for new consumers, and looser standards for established consumers with a shopping history that proves their reliability.⁷⁷

4.6 Restrictions and security measures for delivery services

Reconsidering the results of the evaluation of the risk potential of delivery vulnerabilities (cf. table 3.2 'Evaluation of the risk potential of delivery vulnerabilities'), most of them can be avoided by merchants.

The highest risk is depicted by *Unattended deliveries* and *Reshipping* of orders. With regards to the latter, it is virtually impossible for merchants to do anything against it, since the delivery is received by an unsuspecting person. Even tight security measures, such as an ID check, can't prevent it. Unattended deliveries, however, can be counteracted. To avoid *Unattended secured deliveries*, the option to deliver to drop-off places can be restricted to consumers.⁷⁸ To prevent *Unattended unsecured deliveries*, a signature of the person who receives the delivery can be demanded.⁷⁹

The other delivery vulnerabilities with a medium risk rating can be guarded against as well. *Freight forwarding* can be restricted by a merchant, requiring them to ensure that orders are not shipped to freight forwarding companies. To identify freight forwarders, merchants can either maintain their own list of freight forwarding companies, use lists of freight forwarders that are publicly available, or make use of vendors that provide such a service.^{80,81} *Delivery rerouting* can be prevented by instructing the delivery service to not allow a recipient to reroute of a delivery.

Delivery interception is based on the impersonation of the recipient or a member of the household by the fraudster. Since the delivery agent usually only requires a signature of the person who takes over the delivery, the identity of the person is not verified.⁸² To prevent this, delivery services offer an additional, fee-based service that involves an ID check of the recipient with the simultaneous restriction that a delivery is only handed over to the stated addressee.^{83,84}

In general, the usage of tracking numbers for all orders is recommended.⁸⁵ It allows merchants to stay informed about the whereabouts of a delivery, and can help to protect

⁷⁶[135], pp.77–78.

⁷⁷[94], p.45.

⁷⁸[98], p.3.

⁷⁹[101].

⁸⁰[30], pp.158–160.

⁸¹[91].

⁸²[86], p.34.

⁸³[89].

⁸⁴[90].

⁸⁵[108].

merchants in cases of chargebacks.⁸⁶

Some of these security measures depend on how a delivery is shipped and the corresponding delivery options (such as the signature requirement of the recipient or the restriction of rerouting). They have to be carried out by the delivery service upon the instructions of the merchant, and are often with associated costs. Other measures are the area of responsibility of the merchant (such as the shipment to freight forwarders).

Similar to a consumer-specific risk management regarding the restriction of payment methods, the restriction of delivery options can be done customer-based as well. As the delivery services and options provided by a merchant are one of the main influencing factors for consumers, strict restrictions can result in the loss of potential consumers and transactions.⁸⁷ Considering the value of an order, the risk and value of a consumer (i.e. new consumer or a consumer with a reliable shopping history), the risk of the chosen payment method, and the risk of a certain delivery option allows merchants to determine the overall risk.⁸⁸

⁸⁶[108].

⁸⁷[137], p.182.

⁸⁸[91].

Detecting e-commerce fraud

5.1 General

Fraud prevention can be seen as a passive measure against e-commerce fraud, whereas fraud detection is concerned with actively analysing transactions and identifying fraud attempts immediately and as quickly as possible.^{1,2} Fraud detection must be performed for each and every transaction, as it is unknown whether a transaction is fraudulent or not.³ In layman's terms, the task of fraud detection is to classify each transaction either as legitimate or as fraudulent.⁴

Although it seems to be a binary decision - fraudulent or not fraudulent - it is a much more complex problem. Therefore, it is common to use a scoring model to evaluate a transaction and decide how a transaction should be handled further based on its score. This is described in more detail in 5.1.1 'Transaction scoring'.

Various methods for fraud detection are available, where each is able to detect different kinds of fraud; therefore, they should be used complementary.⁵ Each method has advantages and disadvantages and vary with regard to accuracy, thus combining multiple systems results in a more accurate and effective fraud detection system.^{6,7} The various methods are described in further detail in the respective subchapters: 5.2 'Manual review', 5.3 'Information provider', and 5.4 'Data analysis'.

¹[105], p.236.

²[107], p.315.

³[106], p.235.

⁴[138], p.193.

⁵[60], pp.269–270.

⁶[139], p.3631.

⁷[60], pp.263–264.

The accuracy of a fraud detection system can be depicted with the following rates, illustrated in table 5.1^{8,9,10}:

- TP (True positives): Number of correctly classified fraudulent transactions
- TN (True negatives): Number of correctly classified legitimate transactions
- FP (False positives): Number of legitimate transactions wrongly classified as fraudulent
- FN (False negatives): Number of fraudulent transactions wrongly classified as legitimate

		Transaction	
		Legitimate	Fraudulent
Classification result	Legitimate	TN	FN
	Fraudulent	FP	TP

Table 5.1: Accuracy rates of a fraud detection system¹¹

The objective of fraud detection systems is to maximize the TP and TN rates while minimizing the FP and FN rates.¹² Both of the latter cases result in costs: Cases of FN result in direct losses (as fraud attempts stay undetected and are completed successfully), while cases of FP either generate false alarms, as a result, generate costs for reviewing these transactions, or result in losses by denying transactions to legitimate consumers.¹³ Costs of and losses generated by fraud detection systems are further discussed in 5.1.2 'Costs'.

Fraudsters are adaptive and try to find ways to circumvent detection measures.¹⁴ Therefore, fraud detection systems must continuously evolve to be able to detect new fraud strategies.¹⁵ This challenge as well as other challenges faced by fraud detection systems are discussed in 5.1.3 'Challenges'.

⁸[140], p.13058.

⁹[141], pp.6074–6075.

¹⁰[138], pp.193–194.

¹¹[138], pp.193–194.

¹²[142], p.750.

¹³[143], p.495.

¹⁴[144], p.354.

¹⁵[106], p.235.

5.1.1 Transaction scoring

A *transaction score*, also termed as a *risk score* or *suspicion score*, is a value calculated by a scoring engine based on the inputs of the fraud detection systems.^{16,17} Each fraud detection system determines a certain score, and the combined score indicates the likelihood of a transaction being a fraud attempt: The higher the score, the higher the suspicion.^{18,19}

Such a system can either be installed in-house, calculating a transaction score by combining information retrieved from (internal or external) fraud detection systems, or the whole system can be outsourced to specialized vendors of scoring services.²⁰

The advantage of such a system is that a binary classification would either flag a transaction as fraudulent or legitimate, while the calculated transaction score indicates the degree of risk or suspicion.²¹ This triggers certain actions based on the level of the score, and enables to prioritize further investigations in the case of restricted resources.^{22,23}

Weighting of the various indicators and fraud detection systems respectively allows the score to be more accurately determined.^{24,25} For example, while the usage of different billing and shipping addresses may only slightly increase the score, an IP address from a high-risk country may significantly increase the score. The same applies to the individual fraud detection systems as well: the score of one fraud detection system can have more weight than the score from another system.

Based on the transaction score, further actions can be triggered: If the score is below a certain threshold, the transaction is considered as legitimate and the transaction is further processed.²⁶ If the score is above a certain threshold, the transaction is considered as fraud and rejected immediately.²⁷ If the score is between these two thresholds, it can be flagged as suspicious for further manual review.²⁸ Such a scoring process can vary based on the requirements of a merchant. Alternatively, it can be defined that a transaction is never rejected, but flagged for further review.

¹⁶[63], p.11.

¹⁷[106], p.236.

¹⁸[63], p.11.

¹⁹[106], p.236.

²⁰[30], pp.183–189.

²¹[63], p.11.

²²[63], p.11.

²³[105], p.238.

²⁴[65], p.7.

²⁵[63], p.11.

²⁶[65], pp.6–7.

²⁷[65], pp.6–7.

²⁸[65], pp.6–7.

5.1.2 Costs

The misclassification of transactions, i.e. classifying transactions as FN or FP, generates costs which have to be considered when it comes to fraud detection.^{29,30} Fraudulent transactions that are wrongly classified as legitimate result in direct losses.³¹ Legitimate transactions that are wrongly classified as fraudulent either lead to the rejection of a legitimate purchase (and the loss of a sale or even a customer), or at least lead to a flagged transaction.³² A flagged transaction requires a manual review and investigation of the order, which can lead to considerable costs.³³

Therefore, the objective is to minimize the FN and FP rates, and the misclassification costs, consequently.³⁴ Theoretically, the rates can be reduced as low as desired, but with associated implications on effort and costs.³⁵ Reducing the effort of fraud detection leads to an increase of fraudulent transactions, and, consequently, to an increase of direct losses due to fraud.³⁶ An increase of fraud detection efforts leads to a reduction of fraudulent transactions, but to an increase of costs.^{37,38}

Consequently, a suitable compromise is necessary between the costs for detecting fraud and the savings made by detecting fraud attempts.³⁹ Such a compromise must be effective and economic, and a certain amount of fraudulent transactions have to be tolerated.⁴⁰

5.1.3 Challenges

Complexity

The objective of fraudsters is to avoid suspicion and detection of a fraud attempt in order to maximize profit. They behave as legitimate consumers and expect measures to identify their fraud attempts, therefore fraudsters try to outsmart them.⁴¹ This, and their intention to stay unrecognised, adds to the complexity of detecting fraud.⁴² Moreover, indicators of fraud can be overlapping, meaning a legitimate transaction can appear as fraudulent, while a fraudulent transaction can appear as legitimate.⁴³

²⁹[145], pp.305–306.

³⁰[146], p.4.

³¹[143], p.495.

³²[143], p.495.

³³[106], p.236.

³⁴[146], p.4.

³⁵[106], p.237.

³⁶[63], pp.13–14.

³⁷[63], pp.13–14.

³⁸[106], p.237.

³⁹[106], pp.236–237.

⁴⁰[64], p.1722.

⁴¹[147], p.267.

⁴²[148], p.349.

⁴³[149], p.800.

Limited time span

The time to detect fraud is limited in two respects: The processing time to evaluate a transaction and to either accept or reject it is limited, so as to not make it impractical or inconvenient for consumers.⁴⁴ Also, the time that is available to detect fraud is limited until the point in time where a transaction, and subsequently the success of a fraud attempt, can no longer be stopped.⁴⁵ The value of fraud detection is directly related to time, where the immediate detection is of more value than a delayed detection.⁴⁶

Large amounts of data

Depending on the number of transactions, the amount of data that has to be analysed can be substantial. Nevertheless, the processing time is critical: these systems are required to be able to handle and process large volumes of data within a certain time span.⁴⁷

While the amount of data collected by a merchant may be manageable, service providers that are specialized in detecting fraud, such as credit card issuers, are confronted with a large amount of transactions.⁴⁸

Needle in a haystack

While the amount of data that has to be processed can be extensive, the occurrence of fraudulent transactions is relatively rare.^{49,50} Therefore, it can be described as a needle in a haystack, demonstrating the difficulty of uncovering a few fraudulent needles in an overwhelmingly huge haystack of transactions.⁵¹

This unequal proportion of legitimate and fraudulent transactions can result in high FP rates.⁵² Moreover, it is negatively impacting the performance of fraud detection systems that are trained to detect fraud based on existing data due to the imbalance of fraudulent training examples.⁵³

Dynamic nature of fraud

As soon as a fraud detection system is put in place, it already starts to lose effectiveness.⁵⁴ Fraudsters are continuously adapting their strategies and techniques and try to find ways to circumvent fraud detection measures to keep their fraud attempts undetected.⁵⁵ They

⁴⁴[150], p.827.

⁴⁵[60], p.258.

⁴⁶[151], p.249.

⁴⁷[152], p.141.

⁴⁸[141], p.6070.

⁴⁹[148], p.348.

⁵⁰[152], p.141.

⁵¹[150], p.827.

⁵²[152], p.141.

⁵³[152], p.141.

⁵⁴[151], p.250.

⁵⁵[153], pp.60–61.

become increasingly sophisticated over time, requiring more advanced fraud detection systems.⁵⁶ Therefore, fraud detection systems are required to evolve as well.⁵⁷

Noisy data

When e-commerce fraud is successfully perpetrated, it can remain undetected or stay undetected for up to several months (for example, until a legitimate card holder claims a chargeback).⁵⁸ This results in a delay of correctly labelling a transaction or, consequently, mislabelling a transaction, termed as noisy data.^{59,60}

Therefore, as noisy data is virtually unavoidable, fraud detection systems are almost always based on noisy data.⁶¹ It makes learning from the data more difficult and it has a negative impact on the accuracy of fraud detection systems.⁶²

Historic data

The more historical data of a consumer is available, the more accurate the fraud detection.⁶³ Conversely, the challenge arise with new customers as there is no or hardly any data available that can be used for fraud detection.⁶⁴

Another challenge is that not each fraud detection system has the same level of information.⁶⁵ For example, the fraud detection system of a credit card issuer knows about the transaction history of a card holder, but is not in possession of relevant purchase details. The merchant, on the other hand, is aware of the details of a purchase, but has no access to the transaction history of the card holder. This also illustrates how different fraud detection systems can complement each other.

Incomplete information

The data that can be collected is determined by the operating area of the respective party. A merchant can collect all of the information about a customer and the initiated transaction, including past transactions as well.⁶⁶ However, a merchant has no access to the data of the consumer generated at other merchants' sites, or to the payment history of a certain means of payment.⁶⁷ Therefore, merchants need internal as well as external data to be able to detect fraud.⁶⁸

⁵⁶[152], p.141.

⁵⁷[105], p.236.

⁵⁸[141], p.6070.

⁵⁹[141], p.6070.

⁶⁰[48], p.603.

⁶¹[141], p.6070.

⁶²[152], p.141.

⁶³[148], p.354.

⁶⁴[149], p.800.

⁶⁵[154], p.38.

⁶⁶[150], pp.827–828.

⁶⁷[150], p.828.

⁶⁸[148], pp.349–350.

Moreover, in the case of fraud detection methods that depend on past transactions, the required data becomes available over time.⁶⁹ This can be a problem with new fraud detection systems that only have limited data from the onset.⁷⁰

False alarms

As discussed earlier, misclassification costs are important when it comes to fraud detection. Typically, the majority of transactions flagged as suspicious are actually legitimate.⁷¹ Actions required to follow up on flagged transactions generate effort and tend to be costly.⁷² While the objective of a fraud detection system is to maximize the rate of correct detections of fraudulent transactions, an increase of false alarms is common.⁷³

Data privacy issues

As fraud detection systems rely heavily on the usage and storage of data related to customers, it can also raise issues of data privacy.⁷⁴ Besides raising legal issues, if the usage and storage of customer data does not conform to laws, it can also result in a negative customer experience if customers have the feeling that they have to reveal too much private information that they are not willing to disclose.⁷⁵

Exchange of ideas is limited

What makes the development of fraud detection systems even more difficult is that the exchange of ideas regarding fraud detection is limited and often not publicly available.⁷⁶ This is due to security concerns, as it would provide fraudsters the information they need to circumvent detection measures.⁷⁷ Fraud detection methods are usually described in a very formal way using general terms to not reveal sensitive details.⁷⁸ Real-world data, which would be valuable for testing and creating new fraud detection systems, is not publicly available due to privacy concerns as it often contains the personal data of customers.⁷⁹

⁶⁹[152], p.141.

⁷⁰[152], p.141.

⁷¹[141], p.6070.

⁷²[144], p.355.

⁷³[144], p.355.

⁷⁴[60], p.259.

⁷⁵[155], p.435.

⁷⁶[148], p.350.

⁷⁷[106], p.236.

⁷⁸[148], p.350.

⁷⁹[7], p.384.

5.2 Manual review

This fraud detection method consists of manually reviewing transactions.⁸⁰ This is done by using lookup-tools to verify the details of a transaction, checking the historical data of a consumer, if available, and contacting consumers to verify their identity.⁸¹

This method of fraud detection requires a certain amount of human interaction and effort, is time-consuming, and can be costly.⁸² Scaling is a problem, as the only way to encounter a higher number of transactions is with additional resources, i.e. additional staff members to review the orders. The larger the team reviewing the orders, the more the quality of this fraud detection method varies due to different levels of experience and knowledge.⁸³ Additionally, it can negatively impact customer satisfaction, as manual review usually delays the processing of a transaction.⁸⁴

While manual review might be a reasonable method to detect fraud for small merchants, it is not efficient for large merchants with a high volume of transactions to manually review every order.⁸⁵ Additionally, some strategies of fraudsters can not be detected by manual review.⁸⁶

An economical solution to these drawbacks is to only use manual review for transactions that are suspicious or fulfil certain criteria, such as the value of an order exceeding a certain threshold.⁸⁷ Therefore, the combination of manual review with other fraud detection methods that analyse transactions automatically (and filter out orders that are clearly legitimate) is the key to the efficient use of resources, as it focuses on potentially fraudulent transactions.⁸⁸ This way, manual reviews can even be seen as a method of converting transactions that would have potentially been rejected to routinely handled legitimate transactions.⁸⁹

5.3 Information provider

Information providers are external service vendors offering a variety of methods used for fraud detection. It is distinguished between *Data verification provider*, *Credit score provider*, and *Information sharing provider*.

⁸⁰[63], p.8.

⁸¹[30], pp.211–212.

⁸²[63], p.8.

⁸³[30], p.209.

⁸⁴[22], p.530.

⁸⁵[22], p.530.

⁸⁶[63], p.8.

⁸⁷[65], pp.5–6.

⁸⁸[64], p.1722.

⁸⁹[30], p.209.

5.3.1 Data verification provider

By using data verification services, merchants can verify the data provided by consumers. It comprises methods such as address verification, reverse lookups, and geolocation validation.⁹⁰

Prominent among data verification services is the Address Verification System (AVS) for online credit card payments.⁹¹ It is provided by credit card issuers or payment processors and compares the postal code and the first few digits of the address to the data stored in the database.^{92,93} Merchants receive a response indicating a match or mismatch of the data.⁹⁴

AVS is only available in certain regions, and the usage and advantages are limited, especially with respect to international transactions.⁹⁵ Moreover, it is prone to misclassifying data when card holders make typing errors while entering data or changing their address, resulting in low verification rates.^{96,97}

Reverse lookups can be used to cross-check phone numbers and addresses if they match the name of the consumer.⁹⁸

Geolocation validation can be used to compare the IP address of a consumer and the related location to the provided data.⁹⁹

5.3.2 Credit score provider

Credit bureaus accumulate data from publicly available as well as non-public sources, such as government records, collection agencies, and financial institutions.¹⁰⁰ Using the accumulated data, personalized credit reports are generated.¹⁰¹ Merchants can obtain these reports of their customers, which can be helpful for them in two ways: Firstly, the report contains informations about the respective person, such as the current and previous addresses, allowing the merchant to compare the data entered by a consumer with the data of the credit report.¹⁰² Secondly, the report contains an assessment of the creditworthiness of a consumer, which can also be taken into account when determining the transaction score.¹⁰³

⁹⁰[30], p.129.

⁹¹[63], p.8.

⁹²[156], p.3.

⁹³[30], pp.127–1129.

⁹⁴[157], p.7.

⁹⁵[157], p.7.

⁹⁶[22], p.530.

⁹⁷[156], p.3.

⁹⁸[30], p.166.

⁹⁹[55], p.23.

¹⁰⁰[158], p.60.

¹⁰¹[158], p.60.

¹⁰²[158], p.60.

¹⁰³[158], pp.59–60.

5.3.3 Information sharing provider

Information sharing providers collect and aggregate information provided by merchants and share it among the participating merchants.¹⁰⁴ Various information is collected and shared by the vendors, ranging from lost and stolen documents or payment cards to fraudulently used means of payment and identity-related information about fraudsters.^{105,106,107}

Without information sharing, merchants only have access to the data they have collected; they have no insights into the data or shopping behaviour of a consumer on other merchants' sites. Therefore, they profit from the sharing of information due to the much larger data sets of these information providers and a higher breadth of data.¹⁰⁸ This prevents fraud attempts from the same fraudster, or attempts made with the same fraudulently used documents or means of payment at several merchants.¹⁰⁹

5.4 Data analysis

The availability and access to certain data differentiates between “by operation” systems (using information about the operation) and “by owner” systems (using information about an owner).¹¹⁰ A system using operational information has access and makes use of the data of the operation itself, i.e. the transaction.¹¹¹ These systems, which collect all necessary information about a transaction and can use the data for fraud detection, are operating at the merchant's site. But the information that can be collected is limited to the current and past operations of a consumer. In contrast, a system using information about an owner is based, for example, on the transaction history of a payment card holder.¹¹² Such a system can only be run by a payment card issuer that has access to all payment transactions of a card holder. However, payment card issuers don't have access to all the details of a transaction (besides the necessary parameters to process the payment). Therefore, both systems don't have complete information.¹¹³

Generally, three major methods for e-commerce fraud detection can be distinguished: rule-based expert methods, supervised classification methods, and unsupervised anomaly detection methods.¹¹⁴ These methods can be combined to create hybrid methods. This compensates the downsides of a method and benefits from the combined strength of the used methods.¹¹⁵

¹⁰⁴[30], p.272.

¹⁰⁵[159], pp.291–292.

¹⁰⁶[160].

¹⁰⁷[161].

¹⁰⁸[30], p.273.

¹⁰⁹[49], p.370.

¹¹⁰[150], pp.827–828.

¹¹¹[150], pp.827–828.

¹¹²[150], p.828.

¹¹³[150], p.828.

¹¹⁴[60], p.263.

¹¹⁵[153], pp.55–56.

5.4.1 Rule-based expert methods

These methods are a classical fraud detection approach, used to identify transactions with certain indicators for fraud.^{116,117} The mode of operation is based on a set of rules with the scheme “*if {condition} then {consequence if condition is fulfilled} else {consequence if condition is not fulfilled}*” (where the else part is optional).¹¹⁸ Possible options for consequences are either immediate actions, such as the rejection of a transaction, or the assignment of a certain score indicating the probability of fraudulent behaviour. In the latter case, applying the rules to the details of a transaction allows the calculation of a risk or suspicion score.¹¹⁹ These rules can additionally be weighted, based on the respective probability of fraudulent behaviour.¹²⁰

Rule-based methods are effective at identifying known fraud strategies, but fail at detecting novel strategies.¹²¹

The rules are commonly defined by experts, based on their knowledge and their expertise.¹²² Thus, systems using this approach are denoted as *expert systems*. The underlying idea of expert systems is “*that expertise, which is the vast body of task-specific knowledge, is transferred from a human to a computer*”¹²³. This enables computers to emulate the decision making process obtained by the experts: to make inferences based on the input data and return a specific conclusion.¹²⁴

Relying on a rule-based approach alone can prove to be ineffective, as the rules are likely to be too broad or too strict.¹²⁵ This poses the risk of either not identify a high number of fraudulent attempts (high false negative rate), or of identifying transactions as fraudulent that are indeed legitimate (high false positive rate).¹²⁶

Since the effectiveness of a rule-based expert system is based on the rules defined by the experts, it is also directly dependent on the knowledge and expertise of these experts.¹²⁷ However, since these rules are static in nature, and e-commerce fraud is a dynamic environment, fraudsters are likely to change their strategies and figure out how to circumvent them.¹²⁸ Therefore, a rule-based approach requires a continuous adaptation to changes in fraud strategies, which can result in high maintenance costs.¹²⁹

¹¹⁶[140], p.13058.

¹¹⁷[157], p.5.

¹¹⁸[162], p.11560.

¹¹⁹[147], p.268.

¹²⁰[65], p.6.

¹²¹[60], p.264.

¹²²[60], p.264.

¹²³[163], p.93.

¹²⁴[163], p.94.

¹²⁵[156], p.3.

¹²⁶[156], p.3.

¹²⁷[140], p.13058.

¹²⁸[145], p.295.

¹²⁹[164], p.225.

To overcome the challenge of the dynamic environment, rule-based systems can be extended with self-adapting capabilities to be able to respond to changes accordingly.¹³⁰ This way, a rule-based system can be implemented to learn from past fraudulent transactions that were not correctly identified, as well as from new fraud strategies, allowing it to automatically adjust existing or generate new rules.^{131,132}

5.4.2 Supervised classification methods

Supervised classification methods (or short *supervised methods*) are trained to differentiate between legitimate and fraudulent transactions.¹³³ A set of data, containing labelled transactions (legitimate and fraudulent), is required to construct and train a model consisting of classification rules.¹³⁴ After training, the model is able to assign a suspicion score to incoming transactions, thus classifying a transaction as either fraudulent or legitimate.¹³⁵

As supervised classification methods are trained with examples of past fraud cases, they are good at detecting fraud strategies that have occurred previously, but are less effective or even unusable for detecting novel fraud strategies.^{136,137} Due to the dependency on past labelled data, supervised classification methods are impacted by noisy data, incomplete information, and the unbalanced distribution of excessive legitimate to limited fraudulent transactions (cf. 5.1.3 'Challenges').¹³⁸

Various supervised methods are used for fraud detection; the most popular approaches are listed below:

Rule-based systems are a simple form of supervised classification methods that derive rules from the form *if {condition} then {result}*.¹³⁹ In contrast to expert systems, the rules are derived by an algorithm based on training data.¹⁴⁰

Decision trees are used to classify data.¹⁴¹ Using training data, a tree-like classification model is constructed where each internal node depicts a test on a certain attribute in the data, each branch is an outcome of a certain test, and each leaf equates to a certain class label.^{142,143} Thus, a decision tree can be seen as a sequence of rules that is able to label

¹³⁰[164], p.226.

¹³¹[162], p.11561.

¹³²[145], p.295.

¹³³[105], p.3.

¹³⁴[106], p.239.

¹³⁵[165], pp.260–261.

¹³⁶[60], p.264.

¹³⁷[105], p.3.

¹³⁸[105], p.3.

¹³⁹[106], p.237.

¹⁴⁰[141], p.6071.

¹⁴¹[166], p.2.

¹⁴²[166], p.2.

¹⁴³[158], p.63.

a transaction as fraudulent or legitimate.¹⁴⁴ Decision trees are, due to their structure, easy to understand and interpret.¹⁴⁵

Random forests (or *Decision forests*) are used to overcome the problem of single decision trees, which can be unstable or overly trained to the training data.¹⁴⁶ A random forest consists of a set of decision trees, and aggregates their respective results.¹⁴⁷ The single decision trees are built on separate, independent samples of the training data with a randomly selected subset of attributes of the training data.¹⁴⁸ As a result, random forests are less prone to noisy data and over-fitting to the training data.^{149,150}

Case-based reasoning comprises approaches where the past experience is stored in the form of cases, which represent fraudulent and legitimate transactions.¹⁵¹ For each new case, i.e. new transaction, the stored cases are searched for similar cases and the case with the best fit is selected.^{152,153} Based on the selected case, the new case is classified as fraudulent or legitimate and stored to the existing cases.¹⁵⁴ Therefore, case-based reasoning is able to detect and adapt to previously unknown fraud strategies to a certain extent.¹⁵⁵

Support vector machines are especially useful for binary classifications and highly unbalanced data, both of which apply to e-commerce fraud detection requirements.¹⁵⁶ To classify the data, each transaction of the training data is mapped as a data point to a high-dimensional vector space.¹⁵⁷ The data is separated into two regions by using a so-called hyperplane with either legitimate or fraudulent data points.^{158,159} The separation is determined so that the distance between the two data points of each of the two classes that are nearest to the hyperplane is maximized.¹⁶⁰ New transactions are mapped to the vector space, and depending on the region within which they fall, they are classified as either fraudulent or legitimate.¹⁶¹ Since the decision of the classification is based on the nearness to a certain region, support vector machines are also able to detect previously unknown fraud strategies to some extent.

¹⁴⁴[166], p.2.

¹⁴⁵[167], p.2.

¹⁴⁶[48], p.605.

¹⁴⁷[48], p.605.

¹⁴⁸[48], p.605.

¹⁴⁹[153], p.54.

¹⁵⁰[48], p.605.

¹⁵¹[163], p.96.

¹⁵²[163], p.96.

¹⁵³[168], pp.93–94.

¹⁵⁴[163], p.96.

¹⁵⁵[168], p.93.

¹⁵⁶[48], p.604.

¹⁵⁷[48], p.604.

¹⁵⁸[169], p.36.

¹⁵⁹[149], p.801.

¹⁶⁰[169], p.37.

¹⁶¹[169], pp.36–37.

Neural networks are based on the working principal of the human brain.^{162,163} Like the human brain, neural networks consist of nodes, so-called artificial neurons, and connections between them, the synapses.¹⁶⁴ The artificial neurons have weighted input and output connections, and are organized in three layers: the input layer, hidden layer, and output layer.¹⁶⁵ By training the network, the weights of the synapses are adapted.¹⁶⁶ The neurons react depending on the weights of the input connections and determine a score, passing it to the connected neurons of the adjacent layer.¹⁶⁷ This way, information is passed through the layers, starting from the input layer and ending at the output layer, where the output at the end, in the form of a score, is used to classify a transaction as either fraudulent or legitimate.¹⁶⁸ The network is trained by feeding the input layer with transaction details from the training data and comparing the result from the output layer with the desired output.¹⁶⁹ For each neuron, the error is determined and used to adapt them and the weights of the synapses to approach a state where all transactions from the training data are classified correctly.¹⁷⁰

Bayesian networks can be used for classifying data and identifying patterns.¹⁷¹ These networks are directed acyclic graphs, consisting of nodes and links connecting them in pairs.¹⁷² The nodes correspond to the variables derived from the data: each node has a finite set of states that are mutually exclusive.¹⁷³ The links between the nodes represent the dependence between the variables, thus a node is influenced by a parent node.¹⁷⁴ For each connection, the joint probability can be determined.¹⁷⁵ Therefore, Bayesian networks are not only able to classify a transaction as either fraudulent or legitimate, but can also determine the probability of a transaction belonging to a certain class.¹⁷⁶

Logistic regression is a widely used statistical method for binary classifications, as required for fraud detection.^{177,178} The relationship between a binary variable (the result, i.e. either fraudulent or legitimate) and a set of predictor variables (details of a transaction that can indicate fraud) is used to determine the probability of a transaction being either fraudulent or legitimate due to the presence or absence of certain fraud characteristics.¹⁷⁹

¹⁶²[170], p.34.

¹⁶³[153], p.53.

¹⁶⁴[153], p.53.

¹⁶⁵[170], p.34.

¹⁶⁶[153], p.53.

¹⁶⁷[153], p.53.

¹⁶⁸[170], pp.34–35.

¹⁶⁹[166], p.3.

¹⁷⁰[170], pp.35–36.

¹⁷¹[171], p.154.

¹⁷²[166], pp.4–5.

¹⁷³[172], p.263.

¹⁷⁴[172], p.263.

¹⁷⁵[172], p.263.

¹⁷⁶[169], p.36.

¹⁷⁷[153], pp.52–53.

¹⁷⁸[173], p.15.

¹⁷⁹[153], p.53.

Evolutionary algorithms are based on Darwin’s survival of the fittest principal.¹⁸⁰ As in nature, the objective is to evolve and become better adapted to the environment, which is mimicked by these algorithms.¹⁸¹ Starting with an initial set of rules derived from the training data (the “population”) for classification, new rules are created by combining and mutating existing rules.¹⁸² Out of this set (of “parents” and “offspring”), those rules that perform the classification best are selected (they “survive”), and build the next generation.¹⁸³ By continuing this process, the rules become better adapted at classifying transactions as legitimate or fraudulent.¹⁸⁴ Examples for evolutionary algorithms are *Learning classifier*, *Genetic algorithms*, and *Cultural algorithms*.¹⁸⁵

5.4.3 Unsupervised anomaly detection methods

In contrast to supervised methods, unsupervised anomaly detection methods (or short *unsupervised methods*) don’t require information about the data a priori, i.e. it is not necessary that each transaction from the entire data or the training set be labelled as fraudulent or legitimate.¹⁸⁶ These methods are concerned with detecting unusual salience.¹⁸⁷ Based on the input data, a baseline is determined that represents legitimate behaviour.¹⁸⁸ Ensuing from the baseline, observations are detected that show a significant deviation, namely an anomaly.¹⁸⁹ An anomaly can indicate an unusual transaction, hence a potential case of a fraud attempt.¹⁹⁰

Unsupervised anomaly detection methods are effective in detecting novel fraud strategies, but are not optimized for detecting known fraud strategies.¹⁹¹ Moreover, unsupervised methods are able to detect types of fraud that were previously undiscovered.¹⁹² In contrast to supervised methods, unsupervised methods don’t depend on prior knowledge about the data, i.e. the labelling of transactions, and are not impacted by noisy data or the unequal distribution of fraudulent and legitimate transactions (cf. 5.1.3 ‘Challenges’).¹⁹³

Various approaches for fraud detection exist based on the concept of unsupervised methods:

Outlier detection is a basic form of unsupervised anomaly detection methods.¹⁹⁴ An

¹⁸⁰[174].

¹⁸¹[164], p.226.

¹⁸²[175], p.1.

¹⁸³[175], p.1.

¹⁸⁴[175], p.1.

¹⁸⁵[164], p.226.

¹⁸⁶[165], p.262.

¹⁸⁷[105], p.3.

¹⁸⁸[142], p.750.

¹⁸⁹[106], p.237.

¹⁹⁰[48], p.602.

¹⁹¹[60], p.264.

¹⁹²[142], p.750.

¹⁹³[105], p.6.

¹⁹⁴[176], p.42.

outlier is an observation that deviates significantly from other observations in the data, thus arising suspicion.¹⁹⁵

Clustering segments data into groups with similar characteristics or behaviour, thus identifying and uncovering patterns in the data.^{196,197} It detects local and global outliers.¹⁹⁸ Global outliers are transactions that significantly deviate from the entire data.¹⁹⁹ Local outliers are effective in detecting deviations in heterogeneous subgroups.²⁰⁰ For example, if a consumer, belonging to a certain subgroup with similar spending behaviour, initiates a transaction with a value that is unusual for this group, it is a local outlier and awakes suspicion. The value of the transaction, however, must not be unusual to the entire data set, and is therefore not a global outlier.

Neural networks are applicable for unsupervised methods as well.²⁰¹ Contrary to neural networks for supervised methods, where previous fraud cases are used to teach the neural network to identify similar cases that occur in the future, the unsupervised capabilities of neural networks are used to derive patterns and to cluster and classify the data.²⁰²

Network analysis (or *Link analysis*) is concerned with the relationship and connection of the data.²⁰³ Tightly connected data is grouped together.²⁰⁴ This identifies data with relationships significantly deviating from the relationships of the rest of the data, and it uncovers incriminating relationships between the data.²⁰⁵ The latter is especially useful in revealing organized groups of fraudsters.²⁰⁶

¹⁹⁵[142], p.750.

¹⁹⁶[64], p.1730.

¹⁹⁷[176], p.42.

¹⁹⁸[105], pp.6–7.

¹⁹⁹[105], pp.6–7.

²⁰⁰[105], pp.6–7.

²⁰¹[142], p.750.

²⁰²[64], pp.1722–1723.

²⁰³[177], p.7.

²⁰⁴[146], p.8.

²⁰⁵[148], p.351.

²⁰⁶[178], p.70.

Legal aspects and prosecution of e-commerce fraud

6.1 Legislation in Austria

6.1.1 Legal assessment of the contractual relationship

Every e-commerce transaction is based on a legal transaction, namely a purchase contract, between a merchant, who is offering a good or service, and a consumer, who wants to purchase the offered good or service.

A lawful purchase contract must contain at least the “*essentialia negotii*”, i.e. the statutory minimum requirements.¹ The conclusion of a contract requires the consensus of both contractual partners about the contractual components.² A concluded contract claims “*pacta sunt servanda*”, i.e. the sanctity of the contract, which requires both parties to fulfil their contractual obligations.³

In Austria, legal transactions are regulated in the Austrian Civil Code (“*ABGB - Allgemeines bürgerliches Gesetzbuch*”).

§ 1053 ABGB regulates purchase contracts:

§ 1053 ABGB - Kaufvertrag⁴:

“Durch den Kaufvertrag wird eine Sache um eine bestimmte Summe Geldes einem Andern überlassen. Er gehört, wie der Tausch, zu den Titeln ein Eigentum zu erwerben. Die Erwerbung erfolgt erst durch die Uebergabe des

¹[179], p.820.

²[179], pp.1173–1174.

³[180], pp.37–38.

⁴§ 1053 ABGB [69].

Kaufgegenstandes. Bis zur Uebergabe behält der Verkäufer das Eigenthumsrecht.”

§ 1053 ABGB (English translation) - Purchase contract⁵:

“By a purchase contract, one asset is transferred to someone else for a certain amount of money. It is, as the barter, a title to acquire ownership. The acquisition only takes place upon transfer of the object of purchase. Until the transfer, the seller retains ownership.”

In § 1054 ABGB, the requirements of a purchase contract are laid down:

§ 1054 ABGB - Erfordernisse des Kaufvertrages⁶:

“Wie die Einwilligung des Käufers und Verkäufers beschaffen seyn müsse, und welche Sachen gekauft und verkauft werden dürfen, dieses wird nach den Regeln der Verträge überhaupt bestimmt. Der Kaufpreis muß im barem Gelde bestehen, und darf weder unbestimmt, noch gesetzwidrig seyn.”

§ 1054 ABGB (English translation) - Requirements of the purchase contract⁷:

“The provisions relating to contracts in general provide how the agreement of the seller and the purchaser has to be established and which assets can be purchased and sold. The purchase price must consist of cash and must be neither uncertain or illegal.”

The first sentence refers to the general rules of a contract, which are regulated in §§ 861 et seqq. ABGB.⁸

The general rules of a contract comprise statutory provisions of concluding a contract (§§ 861–864a ABGB), the requirements of a valid contract (§§ 865–867 ABGB), the genuine consent to a contract (§§ 869–877 ABGB), and the possibility and legality of a contract (§§ 878–880a ABGB).⁹

§ 861 ABGB addresses the requirements for the conclusion of a contract:

§ 861 ABGB¹⁰:

“Wer sich erklärt, daß er jemanden sein Recht übertragen, das heißt, daß er ihm etwas gestatten, etwas geben, daß er für ihn etwas thun, oder seinetwegen etwas unterlassen wolle, macht ein Versprechen; nimmt aber der Andere das Versprechen gültig an, so kommt durch den übereinstimmenden Willen beyder

⁵[181], p.257.

⁶§ 1054 ABGB [69].

⁷[181], p.257.

⁸[179], pp.1173–1174.

⁹§§ 861 et seqq. ABGB [69].

¹⁰§ 861 ABGB [69].

Theile ein Vertrag zu Stande. So lange die Unterhandlungen dauern, und das Versprechen noch nicht gemacht, oder weder zum voraus, noch nachher angenommen ist, entsteht kein Vertrag.”

§ 861 ABGB (English translation)¹¹:

“Whoever declares that he intends to transfer his right to someone else which means that he will allow or give him something, do something for him or refrain from something to his benefit, makes a promise; however, if the other person validly accepts the promise, a contract is concluded by mutual consent. As long as the negotiations are pending and the promise has not yet been made or has neither been accepted in advance nor afterwards, no contract is established.”

If a merchant does not recognize the deceit by a fraudster, and makes a declaration of intention, the contract is concluded. The conclusion of the contract requires the merchant to perform the service as agreed in the contract.

However, if the merchant realizes that an e-commerce transaction is fraudulent after closing the contract, article § 870 ABGB is of relevance:

§ 870 ABGB¹²:

“Wer von dem anderen Teile durch List oder durch ungerechte und begründete Furcht (§ 55)¹³ zu einem Verträge veranlaßt worden, ist ihn zu halten nicht verbunden.”

§ 870 ABGB (English translation)¹⁴:

“Whoever has been caused to conclude a contract by deceit or unjust and reasonable fear [(§ 55)]¹⁵ by the counterparty is not bound by such contract.”

The fraud attempt of a fraudster aims to deceive by misleading the merchant regarding the true identity and the intention of the fraudster. The deceit is causal for the conclusion of the agreement, as the merchant would not have agreed to the contract if the true nature of the fraud attempt were apparent. Therefore, according to this article, the contract is void.^{16,17} This means that a contract is legally ineffective, and has not even come into existence.¹⁸

Moreover, according to § 874 ABGB, a merchant can theoretically lodge a claim for compensation in the case of deception:

¹¹[181], p.206.

¹²§ 870 ABGB [69].

¹³Repealed ([182])

¹⁴[181], p.209.

¹⁵∅ No effect

¹⁶[183], p.331.

¹⁷[184], p.19.

¹⁸[183], pp.343–344.

§ 874 ABGB¹⁹:

“In jedem Falle muß derjenige, welcher einen Vertrag durch List oder ungerechte Furcht bewirkt hat, für die nachtheiligen Folgen Genugthuung leisten.”

§ 874 ABGB (English translation)²⁰:

“Whoever caused a contract by way of deceit or unjust fear is liable in any event to provide satisfaction for the negative consequences.”

6.1.2 Criminal offences

The offences of relevance regarding e-commerce fraud are structured in three categories: (1) Offences of fraud, (2) Offences concerned with unlawful usage of non-cash means of payment, and (3) Offences related to the unlawful acquisition of data used to perpetrate fraud.

Offences of fraud

Fraud is an offence against property, as the deception of the fraudster is aimed at the victim of the fraud to either damnify themselves or another person. Offences against property are regulated in the Austrian Criminal Code (*“StGB - Strafgesetzbuch”*).²¹

The general form of fraud is regulated in § 146 StGB:

§ 146 StGB - Betrug²²:

“Wer mit dem Vorsatz, durch das Verhalten des Getäuschten sich oder einen Dritten unrechtmäßig zu bereichern, jemanden durch Täuschung über Tatsachen zu einer Handlung, Duldung oder Unterlassung verleitet, die diesen oder einen anderen am Vermögen schädigt, ist mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.”

§ 146 StGB (English translation) - Fraud²³:

“Any person who by deceiving another about material facts causes the person to do, tolerate or omit an act which causes financial or other material loss to the other person or to a third person and who has the intention to gain an unlawful material benefit for himself, herself, or a third person is liable to imprisonment for up to six months or a fine not exceeding 360 penalty units.”

It consists of five elements of an offence that are causally related: (1) The deceit of the victim, (2) causing a misconception of the victim, (3) inducing the victim to a disposal of

¹⁹§ 874 ABGB [69].

²⁰[181], p.210.

²¹[185].

²²§ 146 StGB [41].

²³[42], p.190.

property, (4) which leads to a financial or material loss, (5) and the gain of an unlawful material benefit for the offender or a third person.²⁴

Intention is defined in § 5 StGB:

§ 5 StGB - Vorsatz²⁵:

- “(1) (1) *Vorsätzlich handelt, wer einen Sachverhalt verwirklichen will, der einem gesetzlichen Tatbild entspricht; dazu genügt es, daß der Täter diese Verwirklichung ernstlich für möglich hält und sich mit ihr abfindet.*
- (2) *Der Täter handelt absichtlich, wenn es ihm darauf ankommt, den Umstand oder Erfolg zu verwirklichen, für den das Gesetz absichtliches Handeln voraussetzt.*
- (3) *Der Täter handelt wissentlich, wenn er den Umstand oder Erfolg, für den das Gesetz Wissentlichkeit voraussetzt, nicht bloß für möglich hält, sondern sein Vorliegen oder Eintreten für gewiß hält.”*

§ 5 StGB (English translation) - Intention²⁶:

- “(1) *A person acts with intention if the person means to complete the elements of an offence; to prove intention, it is enough to show that the person is aware of a substantial risk that the offence will occur and, having regard to the circumstances, takes the risk.*
- (2) *A person acts with purpose if the person means to bring about the circumstances or result for which the law requires proof of purpose or direct intention.*
- (3) *A person acts with knowledge if the person considers the existence or occurrence of a circumstance or result for which the law requires proof of knowledge to be certain, and not merely considers the existence or occurrence to be possible.”*

Moreover, in the case of intention, the attempt to commit fraud is already punishable (not only the completed offence), as stated in § 15 (1) StGB:

§ 15 (1) StGB - Strafbarkeit des Versuches²⁷:

“*Die Strafdrohungen gegen vorsätzliches Handeln gelten nicht nur für die vollendete Tat, sondern auch für den Versuch und für jede Beteiligung an einem Versuch.*”

²⁴[186], pp.151–156.

²⁵§ 5 StGB [41].

²⁶[42], p.23.

²⁷§ 15 StGB [41].

§ 15 (1) StGB (English translation) - Liability for attempt²⁸:

“Criminal liability for intentional conduct is not limited to completed offences but also extends to attempts to commit an offence and to any participation in an attempt.”

It is considered to be an attempt from the moment the fraudster commits the deceit and expects the victim to act accordingly.²⁹ Preliminary work up to this point does not fulfil the requirements of an attempt.³⁰ The offence is completed after the occurrence of the damage.³¹ It is considered damage as soon as the victim renders a service and is affected by the lack of compensation.³² The damage equates to the resulting reduction of property directly related to the fraud, while consequential losses, such as dispute fees, are not considered.³³

Of importance is the requirement that it must affect the financial interest of the victim or a third party. A deceit that does not fulfil this requirement is punishable under § 108 StGB (Deception), which affects the rights of a victim (*“Wer einem anderen in seinen Rechten dadurch absichtlich einen Schaden zufügt [...]”*³⁴; English translation: *“Any person who violates the rights of another [...]”*³⁵).

The wording of the law does not specify where the offence takes place; therefore it is applicable to attempts perpetrated both offline and online, which includes e-commerce fraud.

In § 147 StGB, the offence of aggravated fraud is defined:

§ 147 StGB - Schwerer Betrug³⁶:

“(1) Wer einen Betrug begeht, indem er zur Täuschung

1. eine falsche oder verfälschte Urkunde, ein falsches, verfälschtes oder entfremdetes unbares Zahlungsmittel, ausgespähte Daten eines unbaren Zahlungsmittels, falsche oder verfälschte Daten, ein anderes solches Beweismittel oder ein unrichtiges Meßgerät benützt oder

(Anm.: Z 2 aufgehoben durch BGBl. I Nr. 112/2015)

3. sich fälschlich für einen Beamten ausgibt,

ist mit Freiheitsstrafe bis zu drei Jahren zu bestrafen.

²⁸[42], p.29.

²⁹[187], p.253.

³⁰[187], p.253.

³¹[187], p.261.

³²[187], p.255.

³³[185].

³⁴§ 108 StGB [41].

³⁵[42], p.151.

³⁶§ 147 StGB [41].

- (1a) *Ebenso ist zu bestrafen, wer einen Betrug mit mehr als geringem Schaden begeht, indem er über die Anwendung eines verbotenen Wirkstoffs oder einer verbotenen Methode nach der Anlage der Anti-Doping-Konvention, BGBl. Nr. 451/1991, zu Zwecken des Dopings im Sport täuscht.*
- (2) *Ebenso ist zu bestrafen, wer einen Betrug mit einem 5 000 Euro übersteigenden Schaden begeht.*
- (3) *Wer durch die Tat einen 300 000 Euro übersteigenden Schaden herbeiführt, ist mit Freiheitsstrafe von einem bis zu zehn Jahren zu bestrafen.”*

§ 147 StGB (English translation) - Aggravated fraud³⁷:

“(1) Any person who commits a fraud

1. *by using a false or forged legal document, a false, forged or misapplied non-cash means of payment, reconnoitred data relating to non-cash means of payment, false or forged data, by producing another such piece of evidence, or by using an inaccurate meter to deceive, or*
(Note: subpara. 2 repealed, BGBl. I No. 112/2015)

3. *by misrepresenting himself or herself as a government official*

is liable to imprisonment for up to three years.

- (1a) *The same penalty applies to any person who commits a fraud causing more than merely minor damage by deceiving about the use of one of the prohibited substances or methods set out in the Appendix to the Anti-Doping Convention, BGBl. No. 451/1991, for the purpose of doping in sports.*
- (2) *The same penalty applies to any person who commits a fraud involving damages exceeding 5,000 Euro.*
- (3) *Any person who bring about damages exceeding 300,000 Euro through the offence is liable for imprisonment for one to 10 years.”*

Of relevance for e-commerce fraud is § 147 para. 1 subpara. 1 StGB, as in some cases of e-commerce fraud reconnoitred data relating to non-cash means of payment is used. Additionally, it also covers identity fraud, i.e. the usage of fake or forged data. Paragraph 2 is applicable to rare cases of e-commerce fraud with an exceptionally high amount of losses.

It is considered an aggravated fraud with higher penalties due to the additional utilization of means used by a fraudster to make the deceit more credible.³⁸

If fraud is perpetrated commercially, it falls under § 148 StGB:

³⁷[42], p.191.

³⁸[187], p.263.

§ 148 StGB - Gewerbsmäßiger Betrug³⁹:

“Wer einen Betrug gewerbsmäßig begeht, ist mit Freiheitsstrafe bis zu drei Jahren, wer jedoch einen schweren Betrug nach § 147 Abs. 1 bis 2 gewerbsmäßig begeht, ist mit Freiheitsstrafe von sechs Monaten bis zu fünf Jahren zu bestrafen.”

§ 148 StGB (English translation) - Commercial fraud⁴⁰:

“Any person who commits a fraud commercially is liable for imprisonment for up to three years; any person who commits an aggravated fraud under § 147 paras. 1 to 2 commercially is liable to imprisonment for six months to five years.”

What is considered as commercial fraud is defined in § 70 StGB:

§ 70 StGB - Gewerbsmäßige Begehung⁴¹:

“(1) Gewerbsmäßig begeht eine Tat, wer sie in der Absicht ausführt, sich durch ihre wiederkehrende Begehung längere Zeit hindurch ein nicht bloß geringfügiges fortlaufendes Einkommen zu verschaffen, und

1. unter Einsatz besonderer Fähigkeiten oder Mittel handelt, die eine wiederkehrende Begehung nahelegen, oder
2. zwei weitere solche Taten schon im Einzelnen geplant hat oder
3. bereits zwei solche Taten begangen hat oder einmal wegen einer solchen Tat verurteilt worden ist.

(2) Ein nicht bloß geringfügiges fortlaufendes Einkommen ist ein solches, das nach einer jährlichen Durchschnittsbetrachtung monatlich den Betrag von 400 Euro übersteigt.

(3) Eine frühere Tat oder Verurteilung bleibt außer Betracht, wenn seit ihrer Begehung oder Rechtskraft bis zur folgenden Tat mehr als ein Jahr vergangen ist. In diese Frist werden Zeiten, in denen der Täter auf behördliche Anordnung angehalten worden ist, nicht eingerechnet.”

§ 70 StGB (English translation) - Commercial commission (of an offence)⁴²:

“(1) A person commits an offence commercially, if the person commits the offence for the purpose of obtaining a sustained, more than negligible income for the longer term through the repeated commission of the offence, and

³⁹§ 148 StGB [41].

⁴⁰[42], p.192.

⁴¹§ 70 StGB [41].

⁴²[42], p.108.

1. *the person employs specific skills or means in the commission of the offence which suggests that the offence will be committed repeatedly, or*
 2. *the person has detailed plans for the commission of two further offences of this kind, or*
 3. *the person has previously committed two offences of this kind or has been convicted once for an offence of this kind.*
- (2) *A sustained, more than negligible income is any income that exceeds 400 Euros per month on an annual average.*
- (3) *Prior offences and convictions are not taken into consideration if more than one year has passed between when the offence was committed or the judgement obtained legal force, and the following offence. Any time for which the person was under official arrest is not considered in the calculation of this period.”*

As e-commerce fraud is mostly perpetrated by organized groups and “professional” fraudsters, who have and develop special skills and means to perpetrate fraud and most likely tend to repeat their attempts and refine their strategies over time, most cases of e-commerce fraud qualify for the offence of commercial fraud.

Important for the qualification under §§ 146 and 147 StGB is the deceit of a natural person. If the deceit targets an electronic data processing, it falls under § 148a StGB:

§ 148a StGB - Betrügerischer Datenverarbeitungsmissbrauch⁴³:

- “(1) *Wer mit dem Vorsatz, sich oder einen Dritten unrechtmäßig zu bereichern, einen anderen dadurch am Vermögen schädigt, daß er das Ergebnis einer automationsunterstützten Datenverarbeitung durch Gestaltung des Programms, durch Eingabe, Veränderung, Löschung oder Unterdrückung von Daten oder sonst durch Einwirkung auf den Ablauf des Verarbeitungsvorgangs beeinflusst, ist mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.*
- (2) *Wer die Tat gewerbsmäßig begeht oder durch die Tat einen 5 000 Euro übersteigenden Schaden herbeiführt, ist mit Freiheitsstrafe bis zu drei Jahren, wer durch die Tat einen 300 000 Euro übersteigenden Schaden herbeiführt, mit Freiheitsstrafe von einem bis zu zehn Jahren zu bestrafen.”*

§ 148a StGB (English translation) - Fraudulent misuse of data processing⁴⁴:

⁴³§ 148a StGB [41].

⁴⁴[42], p.192.

- “(1) Any person who causes a financial or other material loss to another by interfering with the result of electronic data processing through design of the program, or through the entry, manipulation, deletion, or suppression of data, or through interference with the processing of data and who has the intention to gain an unlawful material benefit for himself, herself, or a third person is liable to imprisonment for up to six months or a fine not exceeding 360 penalty units.
- (2) Any person who commits the offence commercially or who causes damages exceeding 5,000 Euro is liable to imprisonment for up to three years; any person who causes damages exceeding 300,000 Euro through the offence is liable for imprisonment for one to 10 years.”

The fraudulent usage of a credit card online by someone other than the legitimate holder or a person authorized to use the card falls under this article. The fraudster enters the credit card data, which is transferred by the merchants system to the card processor. Hence, the legitimate card holder falls victim to an illegitimate debit (and consequently the credit card issuer, as the card holder is usually protected), and the merchant receives a debit confirmation.⁴⁵ The same applies to payments via bank transfer and e-wallets.

If a natural person were to be deceived by the fraudulent input, § 148a StGB would not be applicable (but §§ 146 or 147 StGB). However, if a natural person were to control the input but not intervene, the automation-supported process due to the deceptive input would not be considered the deception of a human under prevailing opinion.^{46,47} An offence can only qualify for one of these articles; hence, it must be decided on an individual case basis which offence is satisfied.

Offences of unlawful usage of non-cash means of payment

§§ 241a–h StGB are concerned with cashless means of payment.⁴⁸ These are physical, personalized, or transferable means of payment, with protection against fraudulent usage or forgery that can be used for cashless payments or the disbursement of cash.⁴⁹ This includes checks, debit and credit cards, and electronic wallets (not to be confused with e-wallets, as electronic wallets are chip-based).⁵⁰ Of relevance for e-commerce payments are credit and debit cards.

The counterfeiting of non-cash means of payment, their acceptance, transfer and possession, the preparation of counterfeiting, and active repentance in relation to these offences is addressed by §§ 241a–d StGB.⁵¹ These articles are not applicable to e-commerce fraud,

⁴⁵[187], p.267.

⁴⁶13Os2/07d [188].

⁴⁷13Os61/11m [189].

⁴⁸§ 241a–h StGB [41].

⁴⁹§ 74 para. 1 subpara. 10 StGB [41].

⁵⁰[190], p.163.

⁵¹§ 241a–d StGB [41].

as counterfeited credit or debits cards are not usable in online transactions. It is, however, relevant for card-present payments.

§ 241e is concerned with the theft of non-cash means of payment:

§ 241e StGB - Entfremdung unbarer Zahlungsmittel⁵²:

- “(1) Wer sich ein unbares Zahlungsmittel, über das er nicht oder nicht allein verfügen darf, mit dem Vorsatz verschafft, dass er oder ein Dritter durch dessen Verwendung im Rechtsverkehr unrechtmäßig bereichert werde, ist mit Freiheitsstrafe bis zu zwei Jahren zu bestrafen. Ebenso ist zu bestrafen, wer sich ein unbares Zahlungsmittel, über das er nicht oder nicht allein verfügen darf, mit dem Vorsatz verschafft, sich oder einem anderen eine Fälschung unbarer Zahlungsmittel (§ 241a) zu ermöglichen.
- (2) Wer die Tat gewerbsmäßig oder als Mitglied einer kriminellen Vereinigung begeht, ist mit Freiheitsstrafe von sechs Monaten bis zu fünf Jahren zu bestrafen.
- (3) Wer ein unbares Zahlungsmittel, über das er nicht oder nicht allein verfügen darf, mit dem Vorsatz, dessen Verwendung im Rechtsverkehr zu verhindern, vernichtet, beschädigt oder unterdrückt, ist mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bis zu 720 Tagessätzen zu bestrafen.”

§ 241e StGB (English translation) - Theft of non-cash means of payment⁵³:

- “(1) Any person who acquires non-cash means of payment which the person is not authorized to use or not authorized to use by himself or herself alone with the intention that the person or a third person gains an undue advantage from the use of the non-cash means of payment in legal dealings is liable to imprisonment for up to two years. The same penalty applies to any person who acquires a non-cash means of payment which the person is not authorized to use or not authorized to use by himself or herself alone with the intention to enable himself, herself, or another to counterfeit a non-cash means of payment (§ 241a StGB).
- (2) Any person who commits the offence commercially or as a member of a criminal association is liable to imprisonment for six months to five years.
- (3) Any person who destroys, damages, or suppresses a non-cash means of payment which the person is not authorized to use or is not authorized to use by himself or herself alone with the intention to thwarts its use in legal dealings is liable to imprisonment for up to one year or a fine not exceeding 720 penalty units.”

⁵²§ 241e StGB [41].

⁵³[42], p.311.

This article requires that an offender obtains physical possession of the card by stealing or eliciting it from the legitimate account holder or by extortion with the intention to use it for the enrichment of themselves or a third party or to enable counterfeiting of the card.⁵⁴ The statutory offence is in theory relevant for e-commerce fraud; however, fraudsters are usually not involved with physical crimes and prefer to use the payment details required to make a payment online.

The same applies to § 241f StGB, which regulates the acceptance, transfer, or possession of stolen non-cash means of payment:

§ 241f StGB - Annahme, Weitergabe oder Besitz entfremdeter unbarer Zahlungsmittel⁵⁵:

“Wer ein entfremdetes unbares Zahlungsmittel mit dem Vorsatz, dass er oder ein Dritter durch dessen Verwendung unrechtmäßig bereichert werde, oder mit dem Vorsatz, sich oder einem anderen eine Fälschung unbarer Zahlungsmittel (§ 241a) zu ermöglichen, von einem anderen übernimmt, sich oder einem anderen verschafft, befördert, einem anderen überlässt oder sonst besitzt, ist mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bis zu 720 Tagessätzen zu bestrafen.”

§ 241f StGB (English translation) - Acceptance, transfer or possession of stolen non-cash means of payment⁵⁶:

“Any person who obtains from another, acquires for himself, herself, or another, transports, makes available to another or otherwise possesses a stolen non-cash means of payment with the intention that the person or a third person gain an undue advantage from its use or with the intention to enable himself, herself, or another to counterfeit a non-cash means of payment (§ 241a) is liable to imprisonment for up to one year or a fine not exceeding 720 penalty units.”

§ 241g StGB is concerned with active repentance in relation to §§ 241e–f StGB.

Offenses of unlawful data acquisition

§ 241h StGB addresses the phenomenon of “phishing” (unlawful elicitation of payment details of non-cash means of payment) and “skimming” (unlawful capturing of payment details of non-cash means of payment and fabrication of duplicates):

§ 241h Abs. 1 bis 2 StGB - Ausspähen von Daten eines unbaren Zahlungsmittels⁵⁷:

⁵⁴[190], pp.170–171.

⁵⁵§ 241f StGB [41].

⁵⁶[42], p.312.

⁵⁷§ 241h StGB [41].

- “(1) Wer Daten eines unbaren Zahlungsmittels mit dem Vorsatz ausspäht,
1. dass er oder ein Dritter durch deren Verwendung im Rechtsverkehr unrechtmäßig bereichert werde oder
 2. sich oder einem anderen eine Fälschung unbarer Zahlungsmittel (§ 241a) zu ermöglichen,
- ist mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bis zu 720 Tagessätzen zu bestrafen.
- (2) Wer die Tat gewerbsmäßig oder als Mitglied einer kriminellen Vereinigung begeht, ist mit Freiheitsstrafe bis zu drei Jahren zu bestrafen.”

§ 241h para. 1 to 2 StGB (English translation) - Reconnaissance of data of non-cash means of payment⁵⁸:

- “(1) Any person who reconnoitres data of non-cash means of payment with the intention that,
1. the person or a third person gains an undue advantage from their use in legal dealings, or
 2. to enable himself, herself, or another to counterfeit non-cash means of payment (§ 241a)
- is liable for imprisonment for up to one year or a fine not exceeding 720 penalty units.
- (2) Any person who commits the offence commercially or as a member of a criminal association is liable to imprisonment for up to three years.”

Phishing is one way of acquiring payment data that can be used to commit e-commerce fraud. Fraudsters can either operate their own phishing scheme or can acquire the data required for committing their fraud attempts by a third party.

§ 118a StGB is concerned with the unlawful gathering of data by illegally accessing a computer system:

§ 118a StGB - Widerrechtlicher Zugriff auf ein Computersystem⁵⁹:

- “(1) Wer sich zu einem Computersystem, über das er nicht oder nicht allein verfügen darf, oder zu einem Teil eines solchen durch Überwindung einer spezifischen Sicherheitsvorkehrung im Computersystem in der Absicht Zugang verschafft,
1. sich oder einem anderen Unbefugten Kenntnis von personenbezogenen Daten zu verschaffen, deren Kenntnis schutzwürdige Geheimhaltungsinteressen des Betroffenen verletzt, oder

⁵⁸[42], p.313.

⁵⁹§ 118a StGB [41].

2. einem anderen durch die Verwendung von im System gespeicherten und nicht für ihn bestimmten Daten, deren Kenntnis er sich verschafft, oder durch die Verwendung des Computersystems einen Nachteil zuzufügen,

ist mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.

- (2) Wer die Tat in Bezug auf ein Computersystem, das ein wesentlicher Bestandteil der kritischen Infrastruktur (§ 74 Abs. 1 Z 11) ist, begeht, ist mit Freiheitsstrafe bis zu zwei Jahren zu bestrafen.
- (3) Der Täter ist nur mit Ermächtigung des Verletzten zu verfolgen.
- (4) Wer die Tat nach Abs. 1 im Rahmen einer kriminellen Vereinigung begeht, ist mit Freiheitsstrafe bis zu zwei Jahren, wer die Tat nach Abs. 2 im Rahmen einer kriminellen Vereinigung begeht, mit Freiheitsstrafe bis zu drei Jahren zu bestrafen.”

§ 118a StGB (English translation) - Unlawful use of a computer system⁶⁰:

- “(1) Any person who gains access to a computer system, which the person is not authorized to use or not authorized to use by himself or herself, or who partially gains access to a computer system by overcoming specific security settings for the purpose of
1. acquiring knowledge for himself, herself, or another unauthorized person of personal information, knowledge of which violates confidentiality interests worthy of protection, or
 2. causing a detriment to another by using the information which the person gained access that is saved in the computer system and that is not for his or her attention or by using the computer system,
- is liable to imprisonment for up to six months or a fine not exceeding 360 penalty units.
- (2) The person is liable to imprisonment for up to two years if the offence involves a computer system that is a significant component of critical infrastructure (§ 74 para. 1 subpara. 11).
- (3) The perpetrator may only be prosecuted with the authorization of the victim.
- (4) The perpetrator is liable to imprisonment for up to two years if the offence under para. 1 is committed in connection with a criminal association; the person is liable to imprisonment for up to three years if the offence under para. 2 is committed in connection with a criminal association.”

⁶⁰[42], p.162.

Hacking a computer system to retrieve payment or identity-related data can be another way to acquire data that can be used to commit e-commerce fraud. It can be done by either fraudsters themselves or by a third party who is specialized in hacking computer systems and selling the gathered data to fraudsters.

Another way to gather data is to intercept the transmission of information of a computer system or telecommunication, as regulated in §§ 119 and 119a StGB:

§ 119 StGB - Verletzung des Telekommunikationsgeheimnisses⁶¹:

“(1) Wer in der Absicht, sich oder einem anderen Unbefugten vom Inhalt einer im Wege einer Telekommunikation oder eines Computersystems übermittelten und nicht für ihn bestimmten Nachricht Kenntnis zu verschaffen, eine Vorrichtung, die an der Telekommunikationsanlage oder an dem Computersystem angebracht oder sonst empfangsbereit gemacht wurde, benützt, ist mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.

(2) Der Täter ist nur mit Ermächtigung des Verletzten zu verfolgen.”

§ 119 StGB (English translation) - Breach of telecommunication confidentiality⁶²:

“(1) Any person who uses a device that is connected to a telecommunication or computer system or that has otherwise been prepared to receive communication, for the purpose of acquiring knowledge for himself, herself, or for another unauthorized person of a message transmitted by the way of telecommunication or through a computer system and that is not intended for the person is liable to imprisonment for up to six months or a fine not exceeding 360 penalty units.

(2) The perpetrator may only be prosecuted with the authorization of the victim.”

§ 119a StGB - Missbräuchliches Abfangen von Daten⁶³:

“(1) Wer in der Absicht, sich oder einem anderen Unbefugten von im Wege eines Computersystems übermittelten und nicht für ihn bestimmten Daten Kenntnis zu verschaffen und dadurch, dass er die Daten selbst benützt, einem anderen, für den sie nicht bestimmt sind, zugänglich macht oder veröffentlicht, sich oder einem anderen einen Vermögensvorteil zuzuwenden oder einem anderen einen Nachteil zuzufügen, eine Vorrichtung, die an dem Computersystem angebracht oder sonst empfangsbereit

⁶¹§ 119 StGB [41].

⁶²[42], p.163.

⁶³§ 119a StGB [41].

gemacht wurde, benützt oder die elektromagnetische Abstrahlung eines Computersystems auffängt, ist, wenn die Tat nicht nach § 119 mit Strafe bedroht ist, mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.

(2) *Der Täter ist nur mit Ermächtigung des Verletzten zu verfolgen.”*

§ 119a StGB (English translation) - Improper interception of data⁶⁴:

“(1) *Any person who uses a device that is connected to a computer system or that has otherwise been prepared to receive communication, or who collects the electromagnetic irradiation of a computer for the purpose of acquiring knowledge for himself, herself, or for another unauthorized person of data that has been transmitted by a computer system and that is not intended for the person and has the purpose to obtain a financial or other material benefit for himself, herself, or another or causing a detriment to another by using the data himself or herself, by making it available to another, or by publishing it is liable to imprisonment for up to six months or a fine not exceeding 360 penalty units, unless the offence is punishable under § 119.*

(2) *The perpetrator may only be prosecuted with the authorization of the victim.”*

The requirement for these two offences is that the data espionage happens during transmission (otherwise it would require to unlawfully access a system, which would fall under § 118a StGB).⁶⁵

The main difference between § 119 and 119a StGB is that the first article is concerned with the interception of messages, such as an e-mail, while the second article deals with data in general, also including letter or number sequences, such as access data.⁶⁶

It is a possibility that fraudsters independently commit the aforementioned offences to acquire data that can be used to commit e-commerce fraud. However, it is more likely that they rely on the services of specialized criminals who commit these crimes and supply the fraudsters with the gathered data.

Therefore, the dissemination and acquisition of data used to perpetrate e-commerce fraud is highly relevant. The corresponding criminal offence is regulated in § 126c StGB:

§ 126c Abs. 1 StGB - Missbrauch von Computerprogrammen oder Zugangsdaten⁶⁷:

⁶⁴[42], p.164.

⁶⁵[186], p.98.

⁶⁶[187], pp.161–162.

⁶⁷§ 126c StGB [41].

“(1) Wer

1. ein Computerprogramm, das nach seiner besonderen Beschaffenheit ersichtlich zur Begehung eines widerrechtlichen Zugriffs auf ein Computersystem (§ 118a), einer Verletzung des Telekommunikationsgeheimnisses (§ 119), eines missbräuchlichen Abfangens von Daten (§ 119a), einer Datenbeschädigung (§ 126a), einer Störung der Funktionsfähigkeit eines Computersystems (§ 126b) oder eines betrügerischen Datenverarbeitungsmissbrauchs (§ 148a) geschaffen oder adaptiert worden ist, oder eine vergleichbare solche Vorrichtung oder
2. ein Computerpasswort, einen Zugangscode oder vergleichbare Daten, die den Zugriff auf ein Computersystem oder einen Teil davon ermöglichen, mit dem Vorsatz herstellt, einführt, vertreibt, veräußert, sonst zugänglich macht, sich verschafft oder besitzt, dass sie zur Begehung einer der in Z 1 genannten strafbaren Handlungen gebraucht werden, ist mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.”

§ 126c para. 1 StGB (English translation) - Misuse of computer programmes or login data⁶⁸:

“(1) Any person who develops, launches, distributes, sales, gains access to, obtains or possesses

1. a computer program or similar device, which due to its particular nature has been clearly developed or adapted to gain unlawful access to a computer system (§ 118a), to breach telecommunication confidentiality (§ 119), to commit an improper interception of data (§ 119a), to cause damage to electronic data (§ 126a), to disrupt a computer system (§ 126b), or to commit a fraudulent misuse of data processing (§ 148a),
2. a computer password, login, or similar data that enables, in whole or in part, access to a computer system with the intention to use them to commit one of the offences under subpara. 1 is liable to imprisonment for up to six months or a fine not exceeding 360 penalty units.”

Of interest regarding e-commerce fraud is § 148a StGB, if the unlawfully acquired data is used to attempt e-commerce fraud. The article is concerned with preparatory acts to commit other crimes. Therefore, if a fraudster commits crimes under § 126c StGB and § 148a StGB, the conviction under § 148a StGB already compensates § 126c StGB.⁶⁹

⁶⁸[42], p.174.

⁶⁹[187], p.182.

Interestingly, this article does not cover credit and debit card data. In fact, computer passwords or logins are used for online banking and e-wallets, but card data is not considered as such.^{70,71} However, due to the compensation of § 126c StGB by § 148a StGB, the punishment for a fraudster is the same, regardless of how the payment data of the fraudulently used means of payment, used for a fraud attempt that falls under § 148a StGB (credit and debit cards, bank transfers, or e-wallets), was acquired.

Summarization

E-commerce fraud and the mere attempt to commit it are punishable under §§ 146-148a StGB. Aggravating factors are the usage of means to make the deceit more credible, and repeated attempts to commit e-commerce fraud and to be part of an organized association that commits e-commerce fraud.

If a human is the target of a deceit, §§ 146 or 147 StGB are applicable. If the processing of an e-commerce transaction is automatized and human intervention is not foreseen, as is the case in so-called “secure payment procedures”, § 148a applies.⁷² As soon as an online payment is carried out by using credit or debit card data, a bank transfer, or an e-wallet, it falls under § 148a StGB, which applies to the majority of fraudulent transactions.

The victim in cases of e-commerce fraud where credit or debit cards, or an e-wallet is fraudulently used for payment shifts over time. In the beginning, the victim of the fraudster is the legitimate card or account holder, as a debit is made without their authorization. If the fraud is not detected, the merchant performs the contract. The compensation for it, however, is outstanding, as the card or account holder claims a refund for the unauthorized transaction, and is no longer the victim. Consequently, the merchant or the payment facility affected by the fraud have to agree on a settlement, leaving one of them (or both in case of a split of the losses) behind as the victim. In the case of a bank transfer, it is difficult for an account holder to claim a chargeback. Nonetheless, if the claim for a chargeback is successful, the shift of the victim of the fraud would be the same as for credit and debit cards and e-wallets.

Credit and debit card data are legally not considered as access data, and are, therefore, to be treated differently from bank transfers and e-wallets. For a fraudster, who is “specialized” in committing e-commerce fraud, and makes use of third parties to acquire card or access data, the threat of punishment stays the same. However, it makes a difference if fraudsters obtain payment data by themselves, as the threat of punishment for the theft of non-cash means of payment, phishing, and unlawfully gathering data by illegally accessing a computer system or intercepting a communication differs.

⁷⁰[191], p.44.

⁷¹[192], pp.10–11.

⁷²[193], p.200.

6.1.3 Jurisdiction and venue

The penal power over its own territory is an essential characteristic of a sovereign state.⁷³ Traditionally, each sovereign state (1) decides on its own what is declared as punishable, (2) which criminal offences in case of cross-border crimes are prosecuted, and (3) a state only applies their own substantive criminal law.⁷⁴

In §§ 61–67 StGB, the territorial and chronological purview of the Austrian criminal law is regulated.⁷⁵

While the chronological purview is of less importance for e-commerce fraud, the territorial purview is all the more important due to the possible constellations of fraudster and merchant regarding their origin. In the case of cross-border e-commerce fraud, it is necessary to determine whether there is a connecting factor to Austria, which in turn will apply the Austrian criminal law⁷⁶.

The “principle of territory” defines that a criminal offence is chargeable in Austria if it was committed in Austria.⁷⁷ It is specified in § 62 StGB:

§ 62 - Strafbare Handlungen im Inland⁷⁸:

“Die österreichischen Strafgesetze gelten für alle Taten, die im Inland begangen worden sind.”

§ 62 (English translation) - Domestic offences⁷⁹:

“The Austrian criminal laws apply to all offences committed in Austria.”

The definition regarding the determination of where a criminal offence was committed is specified in § 67 para. 2 StGB:

§ 67 (2) - Ort der Tat⁸⁰:

“Eine mit Strafe bedrohte Handlung hat der Täter an jedem Ort begangen, an dem er gehandelt hat oder hätte handeln sollen oder ein dem Tatbild entsprechender Erfolg ganz oder zum Teil eingetreten ist oder nach der Vorstellung des Täters hätte eintreten sollen.”

§ 67 (2) (English translation) - Place of the offence⁸¹:

“An offence has been committed in every location in which the person engaged

⁷³[194], p.42.

⁷⁴[194], p.42.

⁷⁵§§ 61–67 StGB [41].

⁷⁶[195], p.233.

⁷⁷[196], p.13.

⁷⁸§ 62 StGB [41].

⁷⁹[42], p.97.

⁸⁰§ 67 para. 2 StGB [41].

⁸¹[42], p.106.

or ought to have engaged in the prescribed conduct or in the location in which a result element of the offence, in whole or in part, occurred or in the belief of the person should have occurred.”

Therefore, a crime is considered to be committed in Austria if the offender acts on Austrian territory or the success of the criminal act comes into effect in Austria.⁸²

Applying the articles above to e-commerce fraud: if a merchant with a place of business in Austria is targeted by a fraudster, it makes no difference if the fraudster is located in Austria or outside of Austria, as the (expected) success of the criminal effect is in Austria. As for the regulations regarding fraud, it is not necessary that the fraud attempt was successful, the attempt itself to commit fraud is already punishable.⁸³

If the site of crime is outside of Austrian territory, but the offender committed the crime on Austrian territory, the criminal prosecution is determined by the principle of “vicarious criminal justice”, as regulated in § 65 StGB.⁸⁴

§ 65 StGB - Strafbare Handlungen im Ausland, die nur bestraft werden, wenn sie nach den Gesetzen des Tatorts mit Strafe bedroht sind⁸⁵:

“(1) Für andere als die in den §§ 63 und 64 bezeichneten Taten, die im Ausland begangen worden sind, gelten, sofern die Taten auch durch die Gesetze des Tatorts mit Strafe bedroht sind, die österreichischen Strafgesetze:

- 1. wenn der Täter zur Zeit der Tat Österreicher war oder wenn er die österreichische Staatsbürgerschaft später erworben hat und zur Zeit der Einleitung des Strafverfahrens noch besitzt;*
- 2. wenn der Täter zur Zeit der Tat Ausländer war, im Inland betreten wird und aus einem anderen Grund als wegen der Art oder Eigenschaft seiner Tat nicht an das Ausland ausgeliefert werden kann.*

(2) Die Strafe ist so zu bestimmen, daß der Täter in der Gesamtauswirkung nicht ungünstiger gestellt ist als nach dem Gesetz des Tatorts.

(3) Besteht am Ort der Tat keine Strafgewalt, so genügt es, wenn die Tat nach den österreichischen Gesetzen strafbar ist.

(4) Die Strafbarkeit entfällt jedoch:

- 1. wenn die Strafbarkeit der Tat nach den Gesetzen des Tatorts erloschen ist;*

⁸²[194], p.49.

⁸³[194], p.50.

⁸⁴[194], pp.52–53.

⁸⁵§ 65 StGB [41].

2. wenn der Täter von einem Gericht des Staates, in dem die Tat begangen worden ist, rechtskräftig freigesprochen oder sonst außer Verfolgung gesetzt worden ist;
 3. wenn der Täter von einem ausländischen Gericht rechtskräftig verurteilt und die Strafe ganz vollstreckt oder, soweit sie nicht vollstreckt wurde, erlassen worden oder ihre Vollstreckbarkeit nach dem ausländischen Recht verjährt ist;
 4. solange die Vollstreckung der vom ausländischen Gericht verhängten Strafe ganz oder teilweise ausgesetzt ist.
- (5) Nach den österreichischen Gesetzen vorgesehene vorbeugende Maßnahmen sind, wenn die Voraussetzungen hiefür zutreffen, gegen einen Österreicher auch dann anzuordnen, wenn er aus einem der Gründe des vorhergehenden Absatzes im Inland nicht bestraft werden kann.”

§ 65 StGB (English translation) - Offences committed in a foreign country that are only punishable if they are criminalized under the laws of the place where their offence occurred⁸⁶:

- “(1) Austrian criminal laws apply to offences, other than those mentioned in §§ 63 and 64, that have been committed in a foreign country and are punishable under the laws of the place where they occurred:
1. if the perpetrator, at the time of committing the offence, was an Austrian national or if the perpetrator acquired Austrian citizenship after the offence and continuous to hold Austrian citizenship at the time criminal proceedings are instigated;
 2. if the perpetrator, who, at the time of committing the offence, was a foreign national and is apprehended in Austria and cannot be extradited to the foreign country for reasons other than the type or nature of the offence.
- (2) The sentence is to be determined in a way that, in its totality, it is no less favourable for the perpetrator than under the laws of the place where the offence occurred.
- (3) If the place where the offence occurred does not fall under any criminal jurisdiction, it suffices that the offence is punishable under Austrian law.
- (4) The offence is, however, not punishable:
1. if the offence is no longer punishable under the laws of the place where it occurred;
 2. if the perpetrator has been acquitted with legal force by a court in the country in which the offence has been committed or if the prosecution has been discontinued;

⁸⁶[42], pp.104–105.

3. *if the perpetrator has been convicted with legal force by a foreign court and the sentence has been enforced or, if it has not been enforced, has been pardoned or the statutory limitation period of enforcement under the foreign law has lapsed.*
4. *so long as the enforcement of the sentence by a foreign court has been, in whole or in part, suspended.*
- (5) *Preventative measures recognized under Austrian law may, if relevant requirements are met, also be imposed against an Austrian national, if that person cannot be punished in Austria for any of the reasons listed in the previous paragraphs.”*

(The articles §§ 63 and 64 StGB are not relevant for e-commerce fraud, and are, therefore, not discussed in detail - § 63 StGB extends the territorial purview to ships and aircraft under Austrian flag⁸⁷, and § 64 regulates crimes that are prosecuted independently of the prosecution in the country of the place of crime if they violate Austria’s legal interests⁸⁸).

The principle of “vicarious criminal justice” means that the Austrian prosecution strives to extradite an offender and only punishes a crime if the extradition is not realizable or the foreign judiciary does not take any actions.^{89,90}

6.2 Transnational endeavours against fraud

Subsequently, transnational endeavours against fraud with an impact to Austrian legislation regarding e-commerce fraud are discussed.

6.2.1 Convention on Cybercrime (Council of Europe)

The Convention on Cybercrime is an intergovernmental treaty, initiated by the Council of Europe to establish a multinational framework to harmonize legislation and to foster international cooperation in order to deal with cybercrime.⁹¹ The text of the convention was finalized in 2001 and signed by 30 countries in a signing ceremony in November 2001 in Budapest (hence it is also known as the *Budapest Convention*).^{92,93,94} It came into force in July 2004, after the fifth ratification of a country (as regulated in Article 36 of the convention).^{95,96}

⁸⁷[197], p.6.

⁸⁸[194], p.51.

⁸⁹[194], p.52.

⁹⁰[195], p.234.

⁹¹[198], pp.415–416.

⁹²[198], p.416.

⁹³[195], p.231.

⁹⁴[199].

⁹⁵[200], p.12.

⁹⁶[201], pp.542–543.

As stated by the Council of Europe, the Convention on Cybercrime “*is the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security. It also contains a series of powers and procedures such as the search of computer networks and interception. Its main objective [...] is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international co-operation*”⁹⁷.

Over time, further countries joined the treaty, and it gained support from different international organizations, such as Interpol.⁹⁸

Currently, the convention is ratified by 55 countries, 43 of which are members of Council of Europe (Albania, Andorra, Armenia, Austria, Azerbaijan, Belgium, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Georgia, Germany, Greece, Hungary, Iceland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Monaco, Montenegro, Netherlands, Norway, Poland, Portugal, Republic of Moldova, Romania, Serbia, Slovak Republic, Slovenia, Spain, Switzerland, The former Yugoslav Republic of Macedonia, Turkey, Ukraine, and United Kingdom), and 12 of which are non-members of the Council of Europe (Australia, Canada, Chile, Dominican Republic, Israel, Japan, Mauritius, Panama, Senegal, Sri Lanka, Tonga, and the United States of America).⁹⁹

The convention is divided into four chapters¹⁰⁰:

1. Use of terms
2. Measures to be taken at the national level
3. International co-operation
4. Final provisions

The first chapter (Use of terms) is concerned with defining terms used in the convention: computer system, computer data, service provider, and traffic data.¹⁰¹

Chapter 2 (Measures to be taken at the national level) is divided into three sections: (1) Substantive criminal law, (2) Procedural law, and (3) Jurisdiction.^{102,103} Section *Substantive criminal law* is concerned with specifications regarding offences addressed by the convention: Attacks on computer systems and data (Articles 2–6), computer-related

⁹⁷[202].

⁹⁸[198], p.416.

⁹⁹[203].

¹⁰⁰[204].

¹⁰¹[204].

¹⁰²[204].

¹⁰³[205], p.564.

forgery (Article 7), computer-related fraud (Article 8), child pornography (Article 9), copyright infringements (Article 10), and the attempt and abetment to the previously listed offences (Article 11).¹⁰⁴ The section *Procedural law* (Articles 14–21) provides specifications about the scope of procedural provisions, the preservation and seizure of computer data, the preservation and real-time collection of traffic data, and the interception of content data required to pursue the offences of the previous section and other computer-related crimes.¹⁰⁵ The section *Jurisdiction* (Article 22) specifies the jurisdiction in relation to the offences defined in Articles 2–11.¹⁰⁶

Chapter 3 (International co-operation) is divided into two sections: (1) General principles, and (2) Specific provisions.¹⁰⁷ Section *General principles* specifies provisions on how to co-operate in general; regarding legal assistance, extradition, exchange of information and confidentiality.¹⁰⁸ In section *Specific provisions*, specifications for the mutual assistance regarding the interception and preservation of data as well as disclosure and transborder access to it are defined.¹⁰⁹

The last chapter (Final provisions) is concerned with organizational provisions, such as the commencement of the convention, settlement of disputes, or the denunciation.¹¹⁰

The convention was signed by Austria in the signing ceremony on 23.11.2001, ratified on 13.06.2002, and came into force on 1.10.2002.¹¹¹ The transposition into Austrian law was carried out with the law amending criminal law in 2002.¹¹²

With regard to e-commerce fraud, Article 8 is of particular relevance:

Article 8 - Computer-related fraud¹¹³:

“Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:

- a any input, alteration, deletion or suppression of computer data,*
- b any interference with the functioning of a computer system,*

with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.”

¹⁰⁴[204].

¹⁰⁵[204].

¹⁰⁶[204].

¹⁰⁷[204].

¹⁰⁸[204].

¹⁰⁹[204].

¹¹⁰[204].

¹¹¹[203].

¹¹²[195], p.231.

¹¹³[204].

To be compliant with the specifications of Article 8, only a minor adaptation was required: *“Im § 148a wird die Wendung „Eingabe, Veränderung oder Löschung von Daten“ durch die Wendung „Eingabe, Veränderung, Löschung oder Unterdrückung von Daten“ ersetzt.”*¹¹⁴ (English translation: *In § 148a, the phrase „entry, manipulation, or deletion of data“ is replaced by „entry, manipulation, deletion, or suppression of data“*).

The amendment had partly more extensive effects on the articles of the Austrian Criminal Code discussed above: §§ 118a, 119a and 126c StGB were added anew; § 119 was reformulated, and § 147 was slightly adapted.¹¹⁵

Today, it is still seen as the most comprehensive and important multilateral initiative against cybercrime.^{116,117} It is acknowledged as a tool to harmonize the legislation beyond the European Union.¹¹⁸ According to the Council of Europe, based on an internal list that is not disclosed, more than 100 countries have approximated their legislation to the regulations of the Convention on Cybercrime, either by signing and ratifying the convention or by using the convention when drafting (parts of) their domestic laws.¹¹⁹

Besides the great importance, it also has drawn criticism: Although the Council of Europe was aiming at establishing the convention as a global standard, the number of ratifications does not reflect this, especially since most of the countries are members of the European Union (which have been encouraged by institutions of the European Union to ratify the Convention on Cybercrime).^{120,121} Besides political pressure or economic consequences (such as trading sanctions) to encourage them, there is no possibility to force signatories of the convention to ratify it.^{122,123} It takes a country on average more than five years to ratify the regulations of the convention after signing it, and there is no instrument designated that evaluates whether the regulations are fully implemented.¹²⁴

While the Council of Europe strives to become a global standard and to convince additional countries to ratify it, this simultaneously the complexity of modifications of the convention.¹²⁵ The more countries are involved, each with their own interests, the more difficult it is to coordinate treaty negotiations and to reach an agreement.¹²⁶ But the convention does need an update, as it is criticized for being (at least partly) outdated, due to being drafted back in 2001, and is, therefore, not conceptualized for the cybercrime

¹¹⁴BGBI. I Nr. 134/2002 [206].

¹¹⁵BGBI. I Nr. 134/2002 [206].

¹¹⁶[207], p.502.

¹¹⁷[205], p.565.

¹¹⁸[208], pp.143–144.

¹¹⁹[208], p.143.

¹²⁰[208], p.144.

¹²¹[205], p.566.

¹²²[208], pp.143–144.

¹²³[200], p.14.

¹²⁴[208], pp.144–145.

¹²⁵[205], pp.566–567.

¹²⁶[205], p.567.

developments made since then.^{127,128}

6.2.2 Framework Decision on combating fraud (European Union)

Also in 2001, the *Framework Decision 2001/413/JHA — Combating fraud and counterfeiting of non-cash means of payment* was adopted by the European Union, and the member states were required to implement the provision by 2003.¹²⁹

The intention of the Framework Decision is to harmonize the law of the member states so that “*fraud involving any form of non-cash means of payment (e.g. credit transfer, direct debit, payment card) is recognised as a criminal offence that is punishable by effective, proportionate and dissuasive penalties in all EU countries*”¹³⁰. It is not only concerned with regulations regarding the criminal offences and penalties of fraud and counterfeiting of non-cash means of payment, but also with cooperation among the member states and exchange of information.¹³¹

In Article 1 (a) of the Framework Decision, the term “payment instrument” is defined:

Article 1 (a) - Definition of “payment instrument”¹³²:

“*Payment instrument* shall mean a corporeal instrument, other than legal tender (bank notes and coins), enabling, by its specific nature, alone or in conjunction with another (payment) instrument, the holder or user to transfer money or monetary value, as for example credit cards, eurocheque cards, other cards issued by financial institutions, travellers’ cheques, eurocheques, other cheques and bills of exchange, which is protected against imitation or fraudulent use, for example through design, coding or signature;”

The definition was added to the Austrian Criminal Code¹³³:

§ 74 Abs. 1 Z 10 StGB - Ort der Tat¹³⁴:

“*unbares Zahlungsmittel: jedes personengebundene oder übertragbare körperliche Zahlungsmittel, das den Aussteller erkennen lässt, durch Codierung, Ausgestaltung oder Unterschrift gegen Fälschung oder missbräuchliche Verwendung geschützt ist und im Rechtsverkehr bargeldvertretende Funktion hat oder der Ausgabe von Bargeld dient;*”

§ 74 para. 1 subpara. 10 StGB (English translation)¹³⁵:

¹²⁷[208], p.147.

¹²⁸[205], pp.566–567.

¹²⁹[209].

¹³⁰[210].

¹³¹[209].

¹³²Article 1 (a) [209].

¹³³[211], p.673.

¹³⁴§ 74 para. 1 subpara. 10 StGB [41].

¹³⁵[42], p.114.

“non-cash means of payment: any personal or transferable physical payment method that identifies the issuer, that is protected against forgery or misuse through a code, design, or signature, and that has a cash-substituting function for legal transactions or that serves the disbursement of cash;”

The fraud and forgery of non-cash means of payment is regulated in Article 2:

Article 2 - Offences related to payment instruments¹³⁶:

“Each Member State shall take the necessary measures to ensure that the following conduct is a criminal offence when committed intentionally, at least in respect of credit cards, eurocheque cards, other cards issued by financial institutions, travellers cheques, eurocheques, other cheques and bills of exchange:

- a theft or other unlawful appropriation of a payment instrument;*
- b counterfeiting or falsification of a payment instrument in order for it to be used fraudulently;*
- c receiving, obtaining, transporting, sale or transfer to another person or possession of a stolen or otherwise unlawfully appropriated, or of a counterfeited or falsified payment instrument in order for it to be used fraudulently;*
- d fraudulent use of a stolen or otherwise unlawfully appropriated, or of a counterfeited or falsified payment instrument;”*

The transposition of this article was implemented by adding §§ 241a–g StGB to the Austrian Criminal Code.^{137,138}

In 2016, the European Commission stated that *“available data shows that frauds are still on the rise and affect the trust of the public in digital services and undermine the strengthening of the digital single market. Fraudsters manage to adapt rapidly their modi operandi to evolving technologies and exploit legal loopholes and discrepancies, setting up transnational criminal networks, posing challenges to law enforcement”*¹³⁹. The Framework Decision is focused on physical cards, and does not consider new forms of crime and the development of new technologies that have emerged since then, such as mobile payments or virtual currencies.¹⁴⁰ Therefore, the European Commission has initiated a review of the regulations to combat fraud and counterfeiting of non-cash means of payment in order to adapt and extend it to today’s requirements.^{141,142}

¹³⁶Article 2 [209].

¹³⁷[212], pp.383–384.

¹³⁸[213].

¹³⁹[214].

¹⁴⁰[215].

¹⁴¹[214].

¹⁴²[8], p.66.

Crime-as-a-Service

7.1 Cybercrime and the emergence of Crime-as-a-Service

Cybercrime is defined by Interpol as “*exploiting the speed, convenience and anonymity of the Internet to commit a diverse range of criminal activities that know no borders, either physical or virtual, cause serious harm and pose very real threats to victims worldwide*”¹.

The definition points out the broad range of cybercrime, which is illustrated in figure 7.1: Cybercrime is always *people-related* and *technology-related* to varying degrees.² For example, a crime on the left-hand side in the illustration could be a fraudster sending a mail to unsuspecting people, asking for a payment to provide something in return (which the victims will never receive). In this case, the core crime is only peripherally technology-related.³ On the right-hand side are solely technology-related crimes, for example, if a hacker infests a computer with malware.⁴

The last few years have seen a dramatic increase in cybercrime. People in ever-escalating numbers, turned to cybercrime due to the perceived low risk and the promise of high profits.⁶ What contributed tremendously to its development was the growing commercialization and profit-driven industrialization of the cybercrime economy.⁷ This development resulted in the emergence of a phenomenon termed *Crime-as-a-Service*.⁸

Crime-as-a-Service changed the underground economy towards a thriving criminal industry with a service-based business model that “*drives the digital underground*

¹[216].

²[217], pp.15–16.

³[217], pp.15–16.

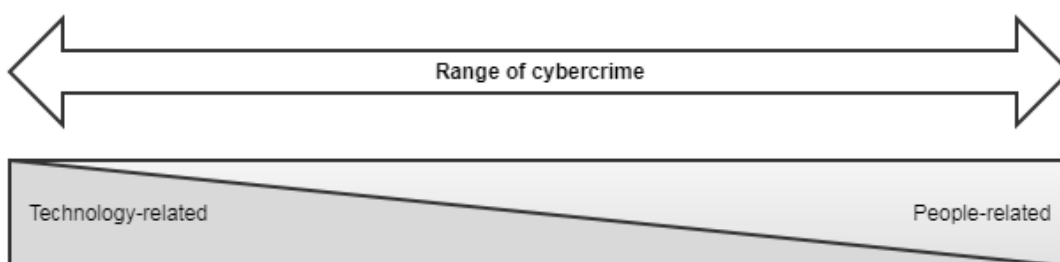
⁴[217], pp.15–16.

⁵Modified from [217], p.15.

⁶[218], p.25.

⁷[50], p.5.

⁸[219], p.2.

Figure 7.1: Range of cybercrime⁵

economy by providing a wide range of commercial services that facilitate almost any type of cybercrime”⁹. Thus, Crime-as-a-Service “grants easy access to criminal products and services, enables a broad base of unskilled, entry-level cybercriminals to launch attacks of a scale and scope disproportionate to their technical capability and asymmetric in terms of risks, costs and profits”¹⁰. Consequently, cybercriminals are offering their services (products, tools, consulting, infrastructure) to other cybercriminals, allowing the first group to monetize their skills, while the latter group is able to operate on a level beyond their capabilities.^{11,12}

Cybercriminals can generally be divided into these two unequally distributed groups: Inexperienced or low-skilled cybercriminals who lack technical expertise and purchase the required skills and services.¹³ They are the larger group but a low impact threat.¹⁴ In contrast, the smaller group consists of highly skilled cybercriminals who are responsible for the most damaging attacks and offer their services to the other group.¹⁵ Crime-as-a-Service has led to a decrease of the ratio of highly skilled cybercriminals due to the ever-increasing number of entry-level, low-skilled participants.¹⁶ This is also reflected in the high number of attacks that are neither sophisticated nor advanced, which account for the majority of attacks.¹⁷

There are two cornerstones of Crime-as-a-Service: specialization and division of labour.¹⁸ Specialization allows cybercriminals to focus on a certain domain, thus becoming increasingly skilled and advanced in that particular area.¹⁹ Providing their expertise in the form of services to other cybercriminals enables them to monetize their expertise.²⁰

⁹[50], p.9.

¹⁰[11], p.7.

¹¹[50], p.19.

¹²[9], p.10.

¹³[50], p.23.

¹⁴[50], p.23.

¹⁵[50], p.23.

¹⁶[218], p.28.

¹⁷[8], p.8.

¹⁸[219], p.2.

¹⁹[219], p.2.

²⁰[8], p.70.

Other cybercriminals profit from this because they do not have to master multiple competencies to cover the whole value chain of an attack on their own.²¹ Instead, due to the division of labour, they purchase the services of the highly skilled cybercriminals.²² Therefore, Crime-as-a-Service diminishes the entry barrier for new participants, as it facilitates the outsourcing of the significant parts of an illicit attack.^{23,24} Moreover, it also allows experienced cybercriminals to focus on their core activities, thus becoming even more specialised and efficient.^{25,26}

The implications of Crime-as-a-Service can be illustrated using the *Cybercrime Trichotomy* (cf. figure 7.2), introduced by Europol.^{27,28} It is “a simplified model which aligns representations of the volume of attackers by their technical capability against the potential profits of an attack and the volume of potential victims by their asset value/security/awareness levels”²⁹.

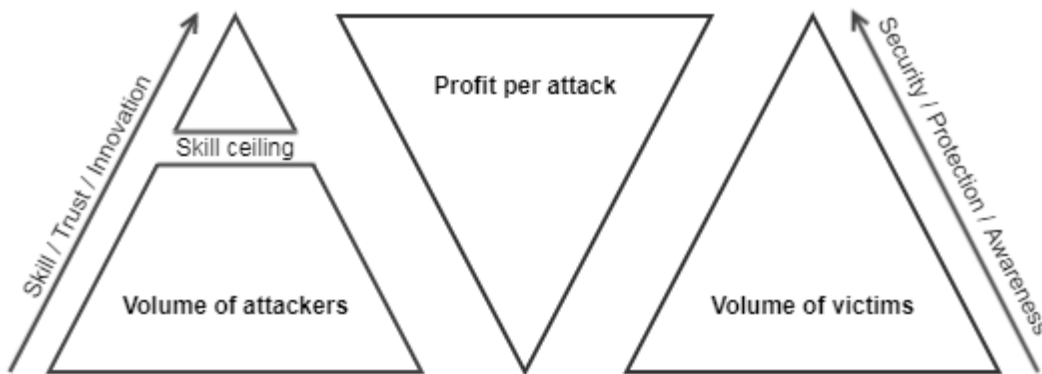


Figure 7.2: Europol's Cybercrime Trichotomy³⁰

The pyramid on the left (*Volume of attackers*) shows that there is a broad base of primarily low-skilled cybercriminals, in addition to a few highly skilled cybercriminals.³¹ The skill ceiling outlines the possibility for low-skilled criminals to make use of the services that high-skilled criminals provide (as-a-Service) to carry out attacks that are above their skill level.³² However, this is limited by the skill ceiling, which requires criminals

²¹[8], p.70.

²²[219], p.2.

²³[10], p.98.

²⁴[220], p.37.

²⁵[50], p.21.

²⁶[221], p.2.

²⁷[11], p.63.

²⁸[8], p.8.

²⁹[11], p.64.

³⁰Modified from [11], p.63.

³¹[11], p.64.

³²[11], p.64.

to develop their own skills and become specialists themselves to be able to overstep the ceiling.³³ The pyramid on the right (*Volume of victims*) analogously shows a broad base of people lacking technical skills with a low level of security and increasingly fewer people with high technical and security skills that are able to protect themselves.³⁴ Additionally, it also demonstrates the value of the victim's assets: it is assumed that the higher the value, the higher the security awareness and level of protection.³⁵ The pyramid in the middle (*Profit per attack*) assumes that the more sophisticated an attack, and the more valuable the victim's assets, the higher the profit.³⁶

Reconsidering the cornerstones of Crime-as-a-Service (specialization and division of labour), the service-based business model allows cybercriminals to act disproportionately above their actual skill level, thus generating higher profits (and causing higher damages).³⁷

Crime-as-a-Service has also paved the way for traditional organised crime groups to enter cybercrime.^{38,39} The service-based economy provides them with the required skills, tools, and services to enhance and facilitate their illicit activities and expand their business models to cyberspace.^{40,41} In general, due to this shift, there is an increasing dependency of traditional crime areas on services provided by the Crime-as-a-Service economy.^{42,43}

The rise of Crime-as-a-Service has also led to a transition of the actors of cybercrime.⁴⁴ Amateur hackers, operating independently or in groups, often seeking a challenge or thrill, have advanced or been replaced over time.⁴⁵ The emergence of the service-based economy allowed cybercrime actors to monetize their skills and expertise, become increasingly specialized and skilled, and make a living as a professional cybercriminal.⁴⁶

Subsequently, money-making entrepreneurial structures have emerged in the form of cybercrime organisations.⁴⁷ These organisations mimic legitimate businesses and are built upon comprehensive business models with strategies to monetize their services and illicit activities.⁴⁸ The income is required to be able to keep the organisation alive (for example, to be able to pay salaries and purchase required services from other organisations).⁴⁹

³³[11], p.64.

³⁴[11], p.64.

³⁵[11], p.64.

³⁶[11], p.64.

³⁷[50], p.7.

³⁸[219], pp.2–3.

³⁹[50], p.11.

⁴⁰[219], pp.2–3.

⁴¹[222], pp.39–40.

⁴²[8], p.48.

⁴³[219], p.4.

⁴⁴[223], p.28.

⁴⁵[223], p.28.

⁴⁶[224], p.12.

⁴⁷[225], p.10.

⁴⁸[9], p.12.

⁴⁹[9], p.12.

They have strict hierarchies, where each member of the organization has a designated role and set of responsibilities, and offer career paths within the organisation.^{50,51}

The hierarchy in these organisations is often similar to that of legitimate IT companies.^{52,53} At the top is the executive suite, usually with few technical but distinct economical skills, which manages the fortunes of the organisation with the intention of maximizing profit.⁵⁴ Below them are tech-savvy members of the organisation, often divided into divisions that are required to fulfil business requirements (for example, a division could be allocated for software development, while another is concerned with the infrastructure or money laundering).⁵⁵ This organisational structure allows highly skilled cybercriminals to focus on their core activities and become even more efficient and specialised, as they don't have to take care of other activities, such as customer acquisition or marketing measures.

Apart from these hierarchical structures, relationships between cybercriminals and cybercrime organizations alike are usually transient, are often transactional, or exist for the purpose of a joint project or a joint campaign.⁵⁶

7.1.1 As-a-Service business models facilitating e-commerce fraud

The service-based cybercrime economy covers practically any service or tool required by cybercriminals to undertake their illicit plans.⁵⁷ Due to the high competition among cybercrime organizations and criminal actors, constant advancement and the expansion of services to arising niches and new criminal areas is guaranteed.⁵⁸

Crime-as-a-Service makes it easy for anyone with sufficient funds to purchase illicit services and goods.⁵⁹ However, access to the services is not only dependent on funds; reputation matters too.⁶⁰ The higher the reputation (and, consequently, the accompanying trust), the easier it is to access more advanced and cutting-edge services and technologies.^{61,62}

The offered services range from various procurement services (for example, acquiring forged documents or data), basic do-it-yourself tools (including step-by-step instructions and support by the developers), consulting services (for example, assistance to set up

⁵⁰[219], p.3.

⁵¹[50], p.20.

⁵²[226], p.6.

⁵³[219], p.3.

⁵⁴[9], pp.11–12.

⁵⁵[219], p.3.

⁵⁶[50], p.21.

⁵⁷[224], p.12.

⁵⁸[224], p.15.

⁵⁹[224], p.12.

⁶⁰[224], p.15.

⁶¹[224], p.12.

⁶²[224], p.15.

a botnet), renting infrastructure, to the contracting of illicit activities (for example, commission of a botnet attack).^{63,64,65}

Infrastructure-as-a-Service, a collective term for all services that provide infrastructure for criminals, is among the key services of the Crime-as-a-Service economy.⁶⁶ In fact, Crime-as-a-Service is highly dependent on Infrastructure-as-a-Service and would not be possible without it.⁶⁷ It comprises various infrastructure services required by cybercriminals, such as the bullet-proof hosting of forums and marketplaces, VPN and proxy services (cf. 7.2.1 'Anonymisation'), and secure storage and bandwidth.^{68,69}

Regarding e-commerce fraud, the scheme of fraudsters is to acquire payment details (like credit card data or account credentials) and use the purchased data to defraud merchants and fraudulently order goods.⁷⁰ To receive the goods, they are reshipped (often several times) via so-called packet mules to obfuscate their tracks.⁷¹ Once received, they are monetised through Internet selling platforms.⁷² E-commerce fraud is therefore mainly facilitated by two illicit services: *Data-as-a-Service* and *Reshipping-as-a-Service*.

Data-as-a-Service

The Data-as-a-Service business model is intended for supplying cybercriminals with data needed by them to conduct their illicit actions.⁷³ The diversity of their crimes (for example, identity fraud, financial fraud, espionage, or e-commerce fraud) directly generates the corresponding diversity of supplied data.⁷⁴ It comprises personal and financial data, such as names, birthdates, payment details (e.g. credit card data), credentials (for e-wallets, social media accounts, or other logins), contact details (such as e-mail addresses, phone numbers, physical addresses), and even forged or stolen documents (e.g. passports, ID cards, or driver's licences), but also other sensitive data such as medical records or confidential corporate information.^{75,76}

With regard to e-commerce fraud, payment card data is a key commodity and, thus, actively traded.⁷⁷ They are either sold by retailers in small, refined batches or distributed by wholesalers in large volume.⁷⁸ The price per payment card or batch strongly depends

⁶³ [225], p.10.

⁶⁴ [9], pp.9–10.

⁶⁵ [227].

⁶⁶ [227].

⁶⁷ [227].

⁶⁸ [50], p.21.

⁶⁹ [223], pp.32–33.

⁷⁰ [50], p.12.

⁷¹ [8], p.29.

⁷² [8], p.29.

⁷³ [225], p.10.

⁷⁴ [225], p.10.

⁷⁵ [50], pp.21–22.

⁷⁶ [228], p.30.

⁷⁷ [50], pp.21–22.

⁷⁸ [11], p.34.

on the respective properties of the cards, for example, rates vary from country to country or by card type (corporate payment card or private payment card).⁷⁹ The more details provided, apart from the card details (for example, the home address of the card holder, the phone number, or the 3D Secure code), the more valuable the data and, correspondingly, the higher the price, as it enables a more legitimate semblance and increases the likelihood that an e-commerce fraud attempt stays undetected.⁸⁰

Data-as-a-Service is highly dependent on other services that are concerned with harvesting data, namely^{81,82,83}:

- Hacking(-as-a-Service)
- Malware(-as-a-Service)
- Phishing(-as-a-Service)

Hacking (also referred to as Cracking) refers to gaining unauthorized access to devices, the intrusion of networks, and causing data breaches.^{84,85} The areas of activity of hacking are broad, and range from simple offences such as gaining access to a device or a social media account, collecting personal information about a target person, to more sophisticated illicit activities such as economic espionage.⁸⁶ With regard to e-commerce fraud, activities with the intention to gain access to and collect sensitive data are of relevance. Large-scale data breaches of private customer data have been a significant data supply source in the last few years, where in some cases millions of records were compromised.^{87,88}

Malware (short for *malicious software*) is one of the key elements of cybercrime and is used for various illicit purposes.⁸⁹ The functionality of malware varies: among other things, it remotely controls infested devices (which are used to build up botnets), damages or negatively impacts the functionality of the devices (i.e. viruses) or locks the devices until a fee is paid (i.e. ransomware), or intercepts or alters data, uses the infested devices to host illegal content, acts as a gateway to load other malware, and steals information.^{90,91} It is common that malware is multifunctional, i.e. that multiple functionalities are

⁷⁹[223], pp.33–34.

⁸⁰[224], p.15.

⁸¹[50], p.36.

⁸²[229], pp.548–549.

⁸³[227].

⁸⁴[230], pp.173–174.

⁸⁵[50], p.48.

⁸⁶[50], p.21.

⁸⁷[11], pp.40–41.

⁸⁸[8], pp.36–37.

⁸⁹[227].

⁹⁰[230], p.184.

⁹¹[50], pp.23–24.

consolidated; nevertheless, it serves a certain primary function.⁹² The majority of the available malware is intended for information stealing, which is of high relevance for e-commerce fraud.⁹³ Any data of potential value is harvested, ranging from logging keystrokes, credit card details, login credentials for social media accounts, e-wallets and online banking, cryptocurrency wallets, and other sensitive user data.^{94,95,96}

Phishing is the “*fraudulent process of attempting to acquire sensitive information, such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication*”⁹⁷. The most common form of phishing is the usage of fraudulent e-mails, often pretending to originate from a finance-related online facility (such as e-wallet or online banking websites), to trick people to disclose sensitive information.^{98,99} While phishing targets a broad victim base, spear-phishing aims at individuals (often high-value targets) in a more personalized way by using private information about the target person to give the appearance of familiarity.^{100,101} Another way to commit phishing is the cloning of merchant websites, where the data of unsuspecting “customers” is collected.^{102,103}

Reshipping-as-a-Service

The Reshipping-as-a-Service scheme is based on three types of actors: *Operators*, *Packet mules* (also termed *Drops* or *Reshipping mules*), and *Stuffers*.^{104,105} An operator creates and runs a reshipping website, i.e., the central component of the scheme.¹⁰⁶ On the one hand, the reshipping website has the purpose to purport the legitimacy of the reshipping service as a professional, legitimate package handling company; on the other hand, it acts as the communication platform between the operator and the packet mules.¹⁰⁷ Operators typically recruit packet mules via job ads offering lucrative work-from-home jobs.¹⁰⁸ They are unsuspecting people, willing to earn some money with a seemingly simple task: receive packages, repackaging the content, put new shipping labels on it, and ship them.¹⁰⁹

⁹²[11], p.18.

⁹³[11], p.20.

⁹⁴[50], p.24.

⁹⁵[11], p.20.

⁹⁶[8], p.19.

⁹⁷[229], p.549.

⁹⁸[230], p.48.

⁹⁹[229], p.549.

¹⁰⁰[231], p.274.

¹⁰¹[8], p.7.

¹⁰²[229], p.549.

¹⁰³[223], pp.35–36.

¹⁰⁴[51], p.1081.

¹⁰⁵[8], p.43.

¹⁰⁶[51], p.1082.

¹⁰⁷[51], p.1082.

¹⁰⁸[51], p.1082.

¹⁰⁹[51], p.1082.

For this duty, they are promised to receive a fixed salary or a commission per package.¹¹⁰ The stuffers are criminals who commit e-commerce fraud and acquire reshipping services to receive the fraudulently obtained goods.¹¹¹

The scheme works as follows (assumed the operator has already recruited a pool of packet mules): The stuffer subscribes to the reshipping website, and gets access to a list of potential packet mules.¹¹² When fraudulently ordering goods (for example, with stolen credit card data), the stuffer chooses one of the packet mules out of the list and uses the address of the packet mule as shipping address.¹¹³ It is common to use the address of the packet mule and the name of the legitimate account holder of the payment means to circumvent fraud detection systems.¹¹⁴ After the order placement, the stuffer adds the order details on the reshipping website to inform the packet mule about the anticipated delivery.¹¹⁵ Upon reception of the order, the packet mule repacks the content, puts a new shipping label on the packet, and reships it.¹¹⁶ Either the operator or the stuffer provide the shipping label (depending on the service level of the reshipping service).¹¹⁷ The shipping address of the label is usually composed of a phony name and an address in the city where the stuffer resides in.¹¹⁸ Finally, the stuffer receives the reshipped package, and resells the goods.¹¹⁹

Depending on the business model, the operator either charges a fixed fee for the service or a certain percentage of the value of the content (up to 50%).¹²⁰ In the case of a percentage, the packet mule is also instructed to take photos and scan the enclosed invoice before repacking, and upload it to the reshipping website, so that the operator knows about the value of the goods.¹²¹

Reshipping-as-a-Service provides two advantages for fraudsters: Firstly, it allows them to receive fraudulently purchased goods in countries where merchants deliberately won't ship to (for example, if it is known as a high-risk country for fraud or due to trading sanctions).¹²² Secondly, it obfuscates their traces and cloaks their identities.¹²³ For a higher level of obfuscation, fraudsters reship an order via several packet mules in succession.^{124,125}

¹¹⁰[51], p.1082.

¹¹¹[51], p.1082.

¹¹²[51], p.1083.

¹¹³[51], p.1083.

¹¹⁴[51], p.1083.

¹¹⁵[51], p.1083.

¹¹⁶[51], p.1083.

¹¹⁷[51], p.1083.

¹¹⁸[51], p.1083.

¹¹⁹[51], p.1083.

¹²⁰[51], p.1086.

¹²¹[51], p.1083.

¹²²[51], p.1082.

¹²³[51], p.1082.

¹²⁴[8], p.29.

¹²⁵[51], p.1086.

Packet mules are victims in a number of ways.¹²⁶ Because they are assisting in fraud, they are likely to be the focus of law enforcement investigations (with potential dire consequences).¹²⁷ Moreover, it is common for reshipping schemes to use packet mules to reship a certain number of packages or for a certain period of time, before contact to them is discontinued by the operator, hence the mules don't receive any money at all.¹²⁸ Furthermore, the operators usually demand personal information and documents (such as a copy of their passport or the driver's licence) of the applying packet mules, which can be, consequently, used to commit identity fraud.¹²⁹

Reshipping-as-a-Service is usually only used for high-value and highly demanded goods.¹³⁰ Due to the service fees of the reshipping service and the costs for the shipping labels, only goods exceeding a certain resale value guarantee a profit for the stuffer.¹³¹ Although the total costs for the reshipping are considerable, fraudsters are dependent on this key service to be able to receive and resell the fraudulently obtained goods; thus, to monetize the illicitly obtained payment information.¹³²

7.2 Facilitating factors of Crime-as-a-Service

Cybercriminals exploit a multitude of legitimate tools and technologies for their illicit criminal gains.¹³³ Some of which are used to facilitate the communication, relationships, and transactions between cybercriminals, while others are used to stay anonymous and obfuscate tracks.^{134,135}

7.2.1 Anonymisation

A common measure of cybercriminals to obfuscate their tracks is the usage of anonymisation tools, which anonymise the IP address to avoid detection and prosecution.^{136,137,138}

Three classes of anonymisation tools can be differentiated: (1) Proxies, (2) VPNs, and (3) the Darknet (i.e. anonymising networks).¹³⁹ These tools can be used standalone or in combination to maximize security.¹⁴⁰

¹²⁶[51], p.1082.

¹²⁷[51], p.1082.

¹²⁸[51], p.1083.

¹²⁹[51], p.1088.

¹³⁰[51], p.1087.

¹³¹[51], p.1086.

¹³²[51], p.1086.

¹³³[50], p.11.

¹³⁴[50], p.11.

¹³⁵[11], p.8.

¹³⁶[11], p.51.

¹³⁷[50], p.55.

¹³⁸[219], p.3.

¹³⁹[50], p.55.

¹⁴⁰[50], p.56.

Proxies

Proxies are the most common, but also most basic anonymisation measures of cybercriminals.¹⁴¹ Proxy servers are intermediaries, transmitting the traffic between a computer and the Internet, as illustrated in figure 7.3. As only the proxy server is visible to the Internet, but not the computer using the proxy server, the computer's IP address is hidden.¹⁴² The most common type of proxies are web proxies which are used to surf the Internet without disclosing the IP address, while other types of proxies allow users to anonymously send mails or use services such as Skype.¹⁴³ Proxy service providers offer their service for free or for a fee; however, it is also a popular method of cybercriminals to use malware and turn infected computers into proxy servers.¹⁴⁴ As it is common for providers to keep logs, which enables to retrace the users behind the proxy servers, proxies do not provide complete anonymity.¹⁴⁵ Therefore, cybercriminals usually pick providers outside their own jurisdiction to complicate prosecution.¹⁴⁶

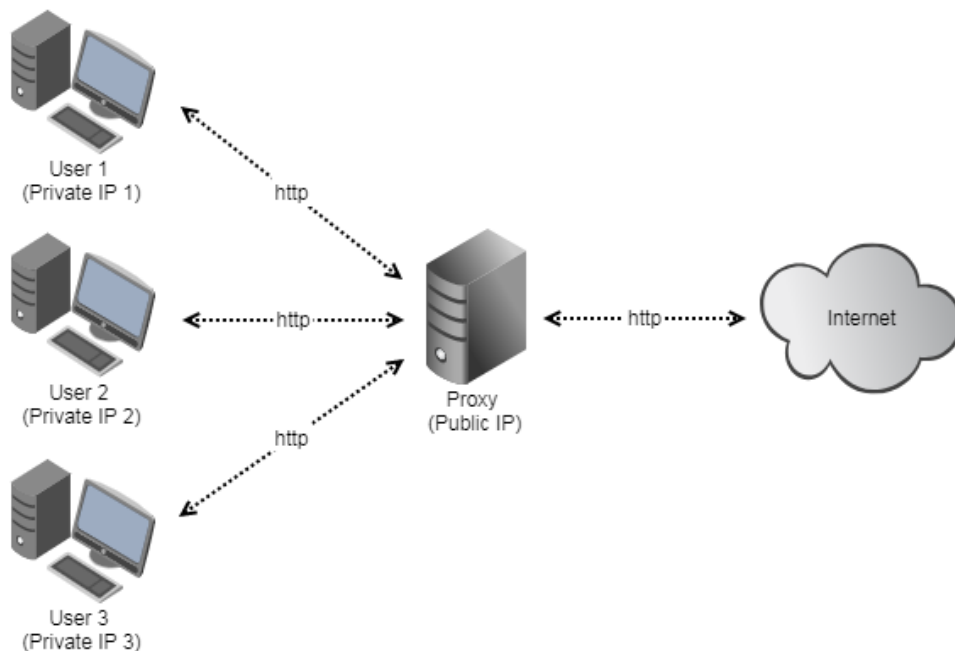


Figure 7.3: Schematic illustration of a proxy server

¹⁴¹[8], p.46.

¹⁴²[232], p.3.

¹⁴³[233], p.33.

¹⁴⁴[233], p.33.

¹⁴⁵[232], p.3.

¹⁴⁶[233], p.33.

VPNs

A VPN (Virtual Private Network) facilitates to access the Internet via an encrypted and secured tunnel that is created between the VPN service and a computer.^{147,148} The whole traffic is transmitted via this tunnel to the VPN service and from there onwards to the Internet (and vice versa), as illustrated in figure 7.4. Therefore, only the IP address of the VPN is externally visible; the IP address of a cybercriminal is hidden and the anonymity is preserved.¹⁴⁹ In contrast to proxies, the whole traffic (not just a certain protocol) is protected when using a VPN connection.¹⁵⁰

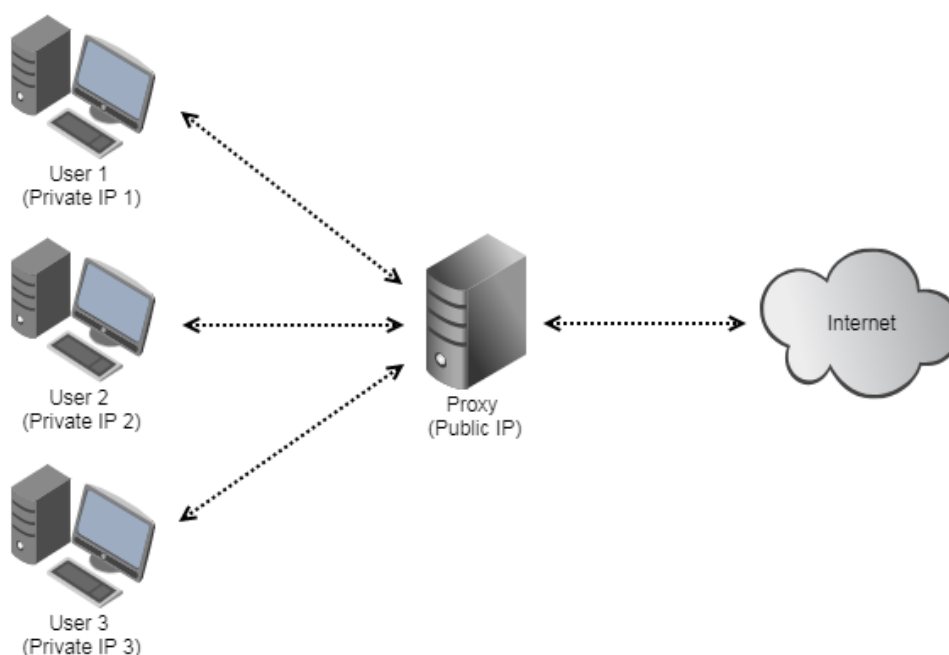


Figure 7.4: Schematic illustration of a VPN

Anonymising networks

Anonymising networks, also collectively referred to as the *Darknet*, have been designed and are intended to protect the personal freedom and privacy of users as well as state security.^{151,152} However, cybercriminals also take advantage of these benefits, as the

¹⁴⁷[232], p.5.

¹⁴⁸[28], pp.158–159.

¹⁴⁹[232], p.5.

¹⁵⁰[232], p.5.

¹⁵¹[8], p.47.

¹⁵²[52], p.22.

Darknet allows them to stay anonymous and conceal their identity.^{153,154}

The operating principle of the aforementioned anonymising networks is based on obfuscating the traces of the traffic^{155,156,157}: This is achieved by distributing the traffic over several nodes of the network, where the nodes are either servers or participating users (depending on the particular concept of the anonymisation network). Each node only knows the inbound node and the outbound node, but not the complete path, as illustrated in figure 7.5. For example, the first node knows about the user (inbound) and the second node (outbound). The second node knows about the first node (inbound), but does not know anything about the user. Additionally, the traffic between the nodes is also encrypted to prevent interception.

To access an anonymising network, a specific software is required.¹⁵⁸ Besides anonymously browsing, the software commonly provides additional functionality, such as anonymously sending messages or sharing files.^{159,160,161}

Moreover, these networks facilitate the anonymous hosting of websites, forums, and marketplaces.¹⁶² As their hosting locations are hidden, they are commonly referred to as *hidden services*.¹⁶³ Hidden services pose a major challenge for law enforcement, since the hosting location is untraceable.¹⁶⁴ Therefore, these anonymising networks prevent any kind of surveillance or content restriction.¹⁶⁵

The most heavily used anonymising network by cybercriminals is *Tor*; distant second and third popular alternatives are *I2P* and *Freenet*.^{166,167}

Tor facilitates the user to browse the Internet anonymously and to host and access websites (i.e. hidden services) within the Tor network.¹⁶⁸ Hidden services have a special pseudo top-level domain, *.onion*, which can only be accessed using the Tor software.¹⁶⁹

The overwhelming majority of Tor users are only using it for anonymous access to the Internet, only about 3-6% of the networks' traffic is related to hidden services.¹⁷⁰ However,

¹⁵³[8], p.47.

¹⁵⁴[52], p.22.

¹⁵⁵[234].

¹⁵⁶[235].

¹⁵⁷[236].

¹⁵⁸[52], p.23.

¹⁵⁹[234].

¹⁶⁰[235].

¹⁶¹[236].

¹⁶²[8], p.47.

¹⁶³[52], p.22.

¹⁶⁴[237], pp.17–18.

¹⁶⁵[237], pp.17–18.

¹⁶⁶[50], p.55.

¹⁶⁷[237], pp.15–16.

¹⁶⁸[237], pp.15–16.

¹⁶⁹[238].

¹⁷⁰[237], p.16.

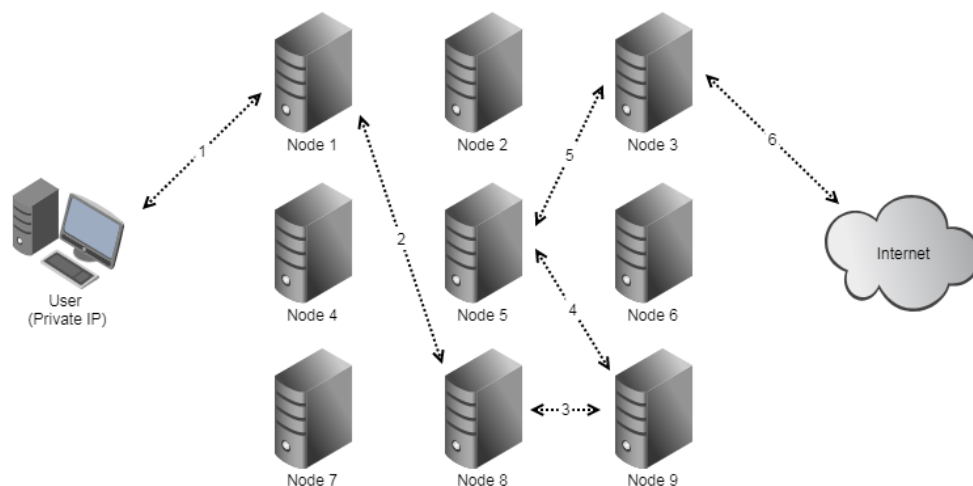


Figure 7.5: Schematic illustration of an anonymising network

it is estimated that more than half of the hidden services in the Darknet are related to illicit activities.^{171,172}

In the Tor network, the traffic is distributed via at least three different servers (referred to as *relays*).¹⁷³ Each user can configure the Tor software to act as a relay.¹⁷⁴

Although challenging for law enforcement, the Tor network (and the Darknet in general) is not impervious. *Operation Onymous*, a joint task force of law enforcement agencies from 21 countries targeted hidden services within the Tor network in November 2014, focusing on illicit marketplaces.^{175,176} More than 600 .onion domains and assets with a total value of more than 1 Million Euros (in form of Bitcoins, cash, drugs, gold and silver) were seized.¹⁷⁷

I2P (abbreviation for *Invisible Internet Project*) also facilitates anonymous Internet access and website hosting (i.e. hidden services).¹⁷⁸ Hidden services, referred to as *cepsites*, are addressed using the pseudo top-level domain .i2p and are only accessible with the I2P software.^{179,180}

¹⁷¹[52], p.22.

¹⁷²[237], p.21.

¹⁷³[239].

¹⁷⁴[240].

¹⁷⁵[241], pp.28–29.

¹⁷⁶[11], p.52.

¹⁷⁷[11], p.52.

¹⁷⁸[235].

¹⁷⁹[242].

¹⁸⁰[243].

In contrast to Tor, each client application of the I2P network acts as a node (referred to as *router*) to distribute the traffic.¹⁸¹ The number of nodes used to obfuscate the traces of traffic is determined based on the security requirements of the communicating participants.¹⁸² The higher the anonymity, the higher the latency, and the lower the throughput.¹⁸³ Also, in contrast to Tor, only dedicated exit nodes can be used to access the Internet, while other nodes only transmit the traffic within the network.¹⁸⁴

Freenet, in contrast to Tor and I2P, is a self-contained network.¹⁸⁵ It can't be used to access resources outside the Freenet, for example the Internet.¹⁸⁶ Instead, it pursues the concept of a distributed datastore: Each node (i.e. participant) of the network contributes bandwidth and a share of their memory space.¹⁸⁷ Uploaded files are encrypted and transmitted over several nodes, stored anywhere within the network and distributed across many nodes.¹⁸⁸ Due to the encryption, users are not able to get to know what files are stored in their memory.¹⁸⁹ As long as a file remains popular, it remains in the Freenet, otherwise it gets deleted.¹⁹⁰

Besides sharing files, the Freenet facilitates hosting and accessing websites within the network (i.e. hidden services), referred to as *frebsites*.¹⁹¹

7.2.2 Forums

Forums are a crucial part of cybercrime and Crime-as-a-Service.¹⁹² The functions are manifold:

- Socializing: Criminals use forums to communicate and discuss with each other.¹⁹³ It plays an essential role in facilitating trust between cybercriminals (which is significantly aggravated due to the inherent virtual and anonymous nature of cybercrime).¹⁹⁴
- Knowledge exchange: Cybercriminals exchange their knowledge on these forums, for example, by publishing guides and tutorials, and by sharing their experience

¹⁸¹[244].

¹⁸²[244].

¹⁸³[244].

¹⁸⁴[244].

¹⁸⁵[245].

¹⁸⁶[245].

¹⁸⁷[245].

¹⁸⁸[245].

¹⁸⁹[245].

¹⁹⁰[245].

¹⁹¹[236].

¹⁹²[52], p.29.

¹⁹³[246], p.71.

¹⁹⁴[247], p.529.

and expertise with others.^{195,196,197}

- Knowledge pooling: Due to the knowledge exchange, forums establish themselves as knowledge bases, contributing to the advancement of the criminal community.^{198,199}
- Meeting points: As cybercrime lacks the opportunity to meet physically, forums function as meeting points where cybercriminals meet and engage with each other and extend their criminal network.^{200,201,202}
- Recruitment: Forums are used to search and recruit co-offenders to jointly carry out offences.^{203,204,205}
- Advertising: Cybercriminals use forums to advertise their products and services.^{206,207}
- Marketplaces: Especially in the early years of cybercrime, forums were heavily used for trading illicit goods and services.²⁰⁸ Although the emergence of dedicated marketplaces led to a shift of trading activities, forums are still used to initiate trading between buyers and sellers.^{209,210}

Forums can be either dedicated to a certain topic (for example, phishing or carding), or cover a broad range of topics.^{211,212} Although some of them are accessible publicly on the Internet, the Darknet (especially Tor) is preferred for hosting underground forums due to the increased anonymity.²¹³

It is common that these forums have restricted access. In general, the higher the level of forum sophistication, the more restricted the access.²¹⁴ Some forums even establish several tiers of access.²¹⁵ To get access to restricted areas of a forum, members must be

¹⁹⁵[247], p.525.

¹⁹⁶[248], p.7.

¹⁹⁷[50], p.19.

¹⁹⁸[246], p.71.

¹⁹⁹[50], p.19.

²⁰⁰[249], p.232.

²⁰¹[221], pp.3–4.

²⁰²[50], p.19.

²⁰³[250], p.36.

²⁰⁴[248], p.5.

²⁰⁵[221], pp.3–4.

²⁰⁶[251], p.16.

²⁰⁷[50], p.19.

²⁰⁸[50], p.19.

²⁰⁹[252], p.54.

²¹⁰[246], p.71.

²¹¹[246], p.71.

²¹²[50], p.19.

²¹³[11], p.11.

²¹⁴[50], p.20.

²¹⁵[251], p.8.

either invited by existing members, or earn reputation and status.^{216,217} A higher status can be earned by contributing to the forum (for example, by publishing tutorials, or engaging in discussions).²¹⁸ In the case of cybercriminals that want to offer their goods and services in a forum, checking processes to validate their offering (for example, by the administrator of a forum) are common to ensure quality and trustworthiness.^{219,220}

7.2.3 Communication

To communicate with each others directly (criminal-to-criminal), cybercriminals use various communication methods. They range from simple e-mail and chat rooms (especially IRC) to messaging services with end-to-end encryption.^{221,222,223}

Although forums play a central role in cybercrime, and usually provide communication options (which are used as well), cybercriminals tend to also communicate outside of the forums.²²⁴ On the one hand, this is due to security concerns, as one can never be sure who has access to the accounts and messages (for example, if an administrator account is compromised by law enforcement).²²⁵ On the other hand, it enables cybercriminals to work independently of the forums in the event of a forum becoming either temporarily or permanently inaccessible (for example, due to technical problems or seizure of the servers by law enforcement).²²⁶

The selection of the communication method is mostly influenced by the following factors: (1) Perception of security and anonymity^{227,228}: For this selection factor, the criteria are, among others, the transmission type (i.e. server-based or P2P), the provided encryption (for example, end-to-end encryption), or the location of servers (because of the underlying jurisdiction); (2) Ease of use and convenience^{229,230}: As for normal users, cybercriminals prefer communication methods that are simple and intuitive to use. Customization options (such as plug-ins for encryption) or localization options (to be able to use a tool in a preferred language) are appreciated as well; (3) Origin and language²³¹: It is common that a language group has preferred communication methods.

²¹⁶[246], p.71.

²¹⁷[50], p.20.

²¹⁸[251], p.7.

²¹⁹[253], p.173.

²²⁰[50], p.20.

²²¹[8], p.11.

²²²[11], p.50.

²²³[251], pp.7–8.

²²⁴[221], pp.3–4.

²²⁵[221], p.4.

²²⁶[221], p.4.

²²⁷[221], p.5.

²²⁸[8], pp.45–46.

²²⁹[221], p.5.

²³⁰[8], pp.45–46.

²³¹[221], p.5.

Table 7.1 shows an overview of the most common messaging services of certain language groups in 2016, according to a recent study.²³²

	1.	2.	3.	4.	5.
English	Skype	Jabber	ICQ	Kik Messenger	AOL Instant Messenger
Russian	Skype	Jabber	ICQ	Telegram	Viber
Chinese	QQ	WeChat	Skype	WhatsApp	Jabber
Spanish	ICQ	Skype	Kik Messenger	Jabber	WhatsApp
French	Jabber	ICQ	Skype	Pidgin	Tox
Arabic	WhatsApp	Skype	AOL Instant Messenger	ICQ	Yahoo! Messenger
Persian	Telegram	Line	Skype	Yahoo! Messenger	Viber

Table 7.1: Commonly used messaging services used by cybercriminals of certain language groups in 2016²³³

Amongst all language groups, Skype is the most commonly used messaging service among cybercriminals.²³⁴ Moreover, Russian-speaking cybercriminals function as role models for other language groups: Russian-speaking cybercriminals are known for their skills, innovativeness and sophistication; hence, other cybercriminals tend to emulate them in order to strengthen their own skills and to facilitate the communication with them.²³⁵ As an example, back in 2012, ICQ was the most used messaging service of Russian-speaking cybercriminals (51.83%), while it was hardly used in other language-groups. Although the usage of ICQ by Russian-speaking cybercriminals decreased significantly until 2016 (21.05%), the usage increased among most of the other language groups.²³⁶

Nowadays, the use of encryption to safeguard communications is common. Cybercriminals are increasingly using secure communication methods with built-in protection (such as Jabber, Telegram, Viber, and WhatsApp, which all provide end-to-end encryption by default or even additional protection features).^{237,238,239} Additionally, the use of encrypted e-mails (typically using PGP²⁴⁰) is increasing as well.²⁴¹

²³²[221], pp.10–16.

²³³[221], pp.10–16.

²³⁴[221], p.17.

²³⁵[221], p.17.

²³⁶[221], p.17.

²³⁷[8], p.46.

²³⁸[221], p.17.

²³⁹[221], pp.7–9.

²⁴⁰PGP, abbreviation for *Pretty Good Privacy*, is an encryption tool that can be used to encrypt and decrypt texts, based on cryptographic public-private key pairs: The public key is used to encrypt a message, which can be decrypted with the private key only. [221], p.8.

²⁴¹[11], p.50.

Another criminal-to-criminal communication method is the usage of draft e-mails: By sharing an account, cybercriminals can write e-mails and save them as a draft; other criminals can read the draft and reply to the message by creating a draft e-mail as well.^{242,243} This way, the tracks of the communication are reduced, as the messages are never sent; thus, preventing the messages from being intercepted.²⁴⁴

7.2.4 Marketplaces

Although forums are used for trading, criminal marketplaces exist where almost any illicit good or service can be purchased.²⁴⁵ The marketplaces can be either specialized (and dedicated to a certain good or service) or have diversified portfolios with goods ranging from drugs, firearms, forged documents, and stolen account credentials to stolen credit card data and services.²⁴⁶ These services can range from different kinds of cybercrime services (such as phishing or DDoS attacks) to contract killings.^{247,248} Moreover, auction houses exist where exploits, vulnerabilities, and stolen data are sold to the highest bidder.²⁴⁹ Another type of marketplaces are specialized shops where the purchase of commodities are increasingly automated.²⁵⁰

Regarding e-commerce fraud, these shops can be used to obtain credit card data or authentication credentials (e.g. e-wallets) in a click-and-buy style.²⁵¹ Certain filter criteria, such as the country of the legitimate account holder or additional related details (i.e., additional information about the identity of an account holder or the 3D Secure code in case of credit cards) facilitate a proper selection of data required to commit e-commerce fraud.^{252,253}

Similarly to legitimate commercial marketplaces, underground markets have established the concept of user reviews and ratings as well.²⁵⁴ Due to the difficulty of verifying the legitimacy of a seller, the reputation of a seller is one of the most important factors in these markets²⁵⁵. Ratings and reviews establish trust and are the basis to build business relations.²⁵⁶ Another way to provide more security with these transactions is the usage of an escrow system. A buyer does not pay the seller directly but rather transfers the

²⁴²[230], p.611.

²⁴³[8], p.45.

²⁴⁴[230], p.611.

²⁴⁵[50], p.19.

²⁴⁶[251], p.4.

²⁴⁷[50], p.20.

²⁴⁸[251], p.4.

²⁴⁹[224], p.14.

²⁵⁰[11], p.34.

²⁵¹[50], p.36.

²⁵²[50], p.36.

²⁵³[254], pp.5-7.

²⁵⁴[50], p.20.

²⁵⁵[50], p.20.

²⁵⁶[50], p.20.

money to an escrow service.²⁵⁷ The escrow service releases the payment to the vendor only if the buyer receives the purchased good or if a purchased service has been carried out.²⁵⁸

As in the legitimate business world, the competition in underground markets is high.²⁵⁹ Therefore, it is common that these marketplaces are service-oriented: customers can collect loyalty points and are offered discounts and money-back guarantees in the case of customer dissatisfaction.²⁶⁰ For example, if the purchased credit card data or authorization credentials were declined when used for a fraud attempt, the buyer can claim a refund.²⁶¹ Sellers commonly provide customer service to buyers to ensure they have a satisfactory experience.²⁶² The sellers who respond to inquiries quickly and provide support to their customers, especially in the case of products or services where a higher degree of skills are required, have a competitive advantage (besides ensuring positive ratings and reviews).²⁶³

According to a study in 2016, narcotics were the most advertised products in these marketplaces, followed by products to commit fraud (such as credit card data, authentication credentials, or stolen or forged documents).²⁶⁴

Silk Road is the best-known representative of these marketplaces; it became known to the broad public due to its shutdown in October 2013 by law enforcement.²⁶⁵ A year later, in November 2014, law enforcement agencies from Europe and the United States carried out *Operation Onymous*, targeting underground markets within the Tor network.²⁶⁶ As a result, a large number of underground marketplaces were shut down, among them *Silk Road 2.0* (the successor of *Silk Road*).^{267,268} Despite the law enforcement's success, cybercriminals still prefer Tor for operating underground marketplaces.²⁶⁹

Not only has law enforcement successes contributed to the vanishing of underground marketplaces, so-called exit scams, hacking attacks (presumably from rivals), and closures for unknown reasons, also occurred.^{270,271} In 2015, *Evolution*, the largest underground marketplace by that time, was shut down by its administrators, which stole all of their customer's Bitcoins (with an estimated value of about 11 Million Euros at that

²⁵⁷[241], p.22.

²⁵⁸[241], p.22.

²⁵⁹[241], p.10.

²⁶⁰[255], p.266.

²⁶¹[255], p.266.

²⁶²[253], p.171.

²⁶³[253], pp.171–172.

²⁶⁴[254], p.3.

²⁶⁵[50], p.20.

²⁶⁶[241], pp.28–29.

²⁶⁷[241], pp.28–29.

²⁶⁸[228], p.29.

²⁶⁹[11], p.11.

²⁷⁰[8], p.47.

²⁷¹[241], pp.28–29.

time).^{272,273} In the same year, another marketplace, *Agora*, one of the largest and oldest marketplaces, closed due to a vulnerability which could have lead to a de-anonymisation of their servers.^{274,275}

As a reaction to the volatility of the underground market economy, caused by law enforcement and the prevalent risk of an unexpected marketplace shutdown, the trend is heading towards decentralization, namely buyers and sellers interact directly with each other (without centralized intermediaries).²⁷⁶ A pioneering approach in this regard is *OpenBazaar*^{277,278,279}: a decentralized marketplaces which is completely based on P2P connections (thus, no centralized servers are necessary). Payments are done using Bitcoin and an escrow services (which is decentralized as well). The decentralization enables users to overcome the weaknesses and vulnerabilities as described before. Due to the decentralized escrow service, exit scams are not feasible, and as there are no centralized servers, it depicts a considerable challenge for law enforcement.

7.2.5 Cryptocurrencies

For purchasing goods and services, cybercriminals make use of various online and offline, ranging from traditional methods such as credit cards or bank transfers to money service bureaus, e-wallets, and cryptocurrencies.²⁸⁰ They tend to choose a payment mean that is convenient and perceived to be low in risk; cybercriminals prefer payments that are as secure and anonymous as possible.^{281,282}

Cryptocurrencies are virtual monetary systems, where units (usually denoted as coins) can be transferred within a network of participants.²⁸³ For this, so-called wallets are used, which are generated using a public-private-key cryptography.²⁸⁴ The public key is used to receive coins, while the private key is used to send coins.²⁸⁵ Transfers are secure, irreversible, and processed instantly and directly, i.e. peer-to-peer between the participants.²⁸⁶ Each transaction is validated and certified by participants of the network using sophisticated algorithms and collected in the so-called blockchain.^{287,288} The

²⁷² [8], p.47.

²⁷³ [254], p.2.

²⁷⁴ [8], p.47.

²⁷⁵ [254], p.3.

²⁷⁶ [52], p.23.

²⁷⁷ [11], p.53.

²⁷⁸ [8], p.46.

²⁷⁹ [254], p.3.

²⁸⁰ [11], p.46.

²⁸¹ [50], p.41.

²⁸² [11], pp.46–47.

²⁸³ [256], p.67.

²⁸⁴ [256], pp.67–68.

²⁸⁵ [257], p.87.

²⁸⁶ [256], p.67.

²⁸⁷ [257], p.86.

²⁸⁸ [256], p.68.

blockchain can be seen as a ledger containing the transactions history of a cryptocurrency.²⁸⁹

The market solely defines the value of a cryptocurrency coin, i.e. by supply and demand; therefore, cryptocurrencies are very volatile and prone to dramatic changes in value.^{290,291}

For most cryptocurrencies, the generation of a wallet is anonymous, thus the participants of a transaction usually remain unidentifiable, as transactions are executed between two wallets (i.e. two public keys).²⁹² The decentralization, i.e., the absence of a central regulatory or governmental control, makes cryptocurrencies resistant to law enforcement disruption or shutdowns; thus, the risk of an exit scam is avoided.²⁹³ Moreover, the security is increased due to the absence of central servers that could be targeted by attacks.^{294,295}

Cryptocurrencies have seen a rise in usage for criminal-to-criminal payments in the last few years; it is currently the most commonly used method of payment between cybercriminals.^{296,297} Presently, there are more than 800 different recorded cryptocurrencies.²⁹⁸ Most prominent among them, and by far most commonly used for criminal-to-criminal transactions, is *Bitcoin*.²⁹⁹

The rise of Bitcoin (and consequently, the rise of cryptocurrencies in general) is believed to be closely related to the emergence and expansion of underground markets.³⁰⁰ Before *Silk Road* came into business, the interest in Bitcoin was negligible.³⁰¹ Because participants of *Silk Road* (and other underground markets) almost exclusively accepted or at least preferred payments made with Bitcoin, it has become the cybercriminals' cryptocurrency of choice, and has demonstrated a rise in interest and value alike.³⁰² The close relation between Bitcoin and underground markets was again noticeable when *Silk Road* was shut down, which led to a huge value drop of Bitcoin.³⁰³

With regards to Bitcoin, and all other cryptocurrencies due to their decentralized nature, the transaction data (i.e. the blockchain) is publicly available, making transactions between wallets (i.e. Bitcoin addresses) transparent.³⁰⁴ Therefore, Bitcoin is considered

²⁸⁹[257], p.87.

²⁹⁰[258], pp.444–445.

²⁹¹[50], p.42.

²⁹²[258], p.446.

²⁹³[50], p.42.

²⁹⁴[50], p.42.

²⁹⁵[258], p.443.

²⁹⁶[8], p.42.

²⁹⁷[228], p.30.

²⁹⁸[259].

²⁹⁹[8], p.42.

³⁰⁰[241], p.30.

³⁰¹[241], p.30.

³⁰²[8], p.42.

³⁰³[241], p.30.

³⁰⁴[8], p.43.

pseudo-anonymous: Transactions are transparent, but wallets can be created without any relation to or information about the account holder.³⁰⁵

To evade the traceability of Bitcoin transactions, specialized laundering services, termed *mixers* or *tumblers*, have emerged.³⁰⁶ These services are used to obfuscate the money flow.³⁰⁷ Criminals transfer their Bitcoins to these services, which collect them in a pool of funds, and transfer the received amount to a new wallet or even a number of wallets (minus a commission fee for the service).^{308,309} The trace of Bitcoins is hereby interrupted.³¹⁰

Additionally, alternate cryptocurrencies have been developed to overcome the disadvantages of Bitcoin: emphasizing more on anonymity and privacy and preventing the traceability of transactions.³¹¹ Nevertheless, none of the alternate cryptocurrencies have managed to compete with the popularity of Bitcoin thus far.³¹²

7.2.6 Online disinhibition effect

In the field of cyberpsychology, the term *online disinhibition effect* denotes the phenomenon that people behave differently online than in the real world.^{313,314}

This effect is based on at least six factors^{315,316}:

- Dissociative anonymity^{317,318}: The Internet allows people to hide or alter some or all of their identity. This can lead to a feeling of dissociation, and consequently to a reduced responsibility for the behaviour online or a denial of responsibility for it at all.
- Invisibility^{319,320}: On the Internet, the presence of a person is often not noticed by others (for example, when a person visits a website). Therefore, people are willing to do things and go to places that they wouldn't usually do or go to in real life.

³⁰⁵[257], p.86.

³⁰⁶[8], p.42.

³⁰⁷[8], p.42.

³⁰⁸[260], p.4.

³⁰⁹[261], pp.12–14.

³¹⁰[237], p.22.

³¹¹[8], pp.42–43.

³¹²[8], p.43.

³¹³[262], pp.321.

³¹⁴[255], p.274.

³¹⁵[263], pp.184–188.

³¹⁶[263], pp.322–324.

³¹⁷[263], pp.184–188.

³¹⁸[263], pp.322–324.

³¹⁹[263], pp.184–188.

³²⁰[263], pp.322–324.

- Asynchronicity^{321,322}: Communication online is often asynchronous (for example, e-mail, message boards, messenger services), which is unnatural in comparison to the conversational flow in real life. This impacts one's train of thought, leading to an aversion of social norms.
- Solipsistic introjection^{323,324}: The absence of face-to-face cues in combination with text-based communication can lead to an internal representation of a communication partner. The perception of this internal represented character is based on the virtual appearance and behaviour of the communication partner on the one hand, and one's personal perception and expectations on the other hand. This can lead to text-based communication taking place inside one's intra-psychic world, i.e. inside one's head.
- Dissociative imagination^{325,326}: Some people see their virtual identities as living in a make-believe dimension, which is dissociated from the responsibilities and norms of the real world. To them, when they leave their computer, their virtual identity keeps on living in the virtual reality; they differentiate between their real identity and virtual identity.
- Minimization of status and authority^{327,328}: In real life, the authority of people influences how other people behave and interact. On the Internet, however, people are equal, and the relations between them feel more like peer relationships. Therefore, the perception of authority is minimized, and people are more willing to misbehave.

Due to the online disinhibition effect, cybercriminals are likely to be bolder and lack fear of law enforcement.³²⁹ This is because of their perception of anonymity, a lack of authority and governance, as well as the physical distance between them and the victims and the site of crime.³³⁰ As a result, it can lead to the notion of operating with impunity, and, consequently, neglecting measures regarding security, encryption, and privacy.³³¹ Organized cybercrime groups tend to use aggressive, confrontational approaches.³³²

³²¹[263], pp.184–188.

³²²[263], pp.322–324.

³²³[263], pp.184–188.

³²⁴[263], pp.322–324.

³²⁵[263], pp.184–188.

³²⁶[263], pp.322–324.

³²⁷[263], pp.184–188.

³²⁸[263], pp.322–324.

³²⁹[219], pp.4–5.

³³⁰[219], pp.4–5.

³³¹[218], p.27.

³³²[11], p.7.

Moreover, inhabiting in illicit environment and being surrounded by like-minded people (cybercriminals, in this case), can alter the perception of wrongdoing: “*If enough people are breaking a law, it stops being regarded as immoral*”³³³.

7.3 Measures against Crime-as-a-Service

Measures against Crime-as-a-Service require a deep understanding of the underlying business models of involved cybercrime organizations.³³⁴ This enables law enforcement to identify counter-measures against the business strategies of cybercrime organizations and actors, as well as the cybercrime economy in its entirety.³³⁵

A core tactic is the disruption of hidden services, thus impacting the criminal economy as a whole.³³⁶ It is common for cybercriminals to have business continuity plans in place to minimize disruption effects (for example, backup servers in case a server is taken down).³³⁷ Therefore, the objective of law enforcement is to cause disruption that can’t be prevented or diminished by continuity plans.³³⁸

To cause disruption, it is necessary to identify key players and key services in the cybercrime economy and their dependencies³³⁹. Key players can either be criminals with a high reputation or a central role, or criminals providing key services.^{340,341} By targeting them, the impact on the criminal community can be considerable, not only because of their absence in the community (and, consequently, the temporary lack of their role or services they provide), but also to alert other criminals.³⁴² Targeting critical infrastructure can also shut down key services, usually run as hidden services.³⁴³

Large-scale attacks on cybercrime organizations and services in recent years resulted in comprehensive disruptions in the cybercrime economy.³⁴⁴ For example, *Operation Onymous* targeted criminal marketplaces, while *Operation Avalanche* targeted a cybercrime organization that was heavily involved in the Crime-as-a-Service business (which provided infrastructure and services, namely for phishing and money laundering).³⁴⁵

These operations have lasting effects on the cybercrime community: It undermines the confidence in the cybercrime economy and fuels distrust, uncertainty, and paranoia among

³³³[255], p.274.

³³⁴[219], p.8.

³³⁵[219], pp.7–8.

³³⁶[8], p.47.

³³⁷[219], p.6.

³³⁸[219], p.6.

³³⁹[50], p.23.

³⁴⁰[8], p.12.

³⁴¹[50], p.23.

³⁴²[50], p.23.

³⁴³[50], p.23.

³⁴⁴[8], p.47.

³⁴⁵[219], p.5.

cybercriminals.^{346,347} Additionally, it demonstrates and reminds cybercriminals that law enforcement is present, and even hidden services and allegedly anonymous cybercriminals are not beyond their reach.³⁴⁸ Moreover, the numerous exit scams are strokes of luck for law enforcement, as they intensify these effects.³⁴⁹

To gather intelligence and obtain criminal evidence, and to learn about future trends and new developments, the cybercrime economy is infiltrated with undercover agents.³⁵⁰ By impersonating cybercriminals, the agents build trust with other cybercriminals and strive to advance to restricted areas.³⁵¹ It is important for undercover agents to act lawfully to make sure that conducted actions are admissible and to ensure the admissibility of gathered evidence.³⁵² The inherent anonymity of the cybercrime economy is a two-edged sword in this case: While the anonymity protects cybercriminals and conceals their real identity, it also aggravates their ability to determine whether someone is an undercover agent.³⁵³

Another way to impact the cybercrime economy and weaken the trust among cybercriminals is the infiltration of undercover agents, who either act as “rippers” (i.e. they act as criminals, offering their products and services, and disappear after receiving the payment) or reveal themselves as law enforcers to demonstrate that law enforcement is present.³⁵⁴ Another method is to target the reputation of key players.^{355,356} For example, by destroying the reputation of sellers with bad reviews and ratings from undercover agents, their business model can be permanently damaged.^{357,358}

The identification of choke points allows law enforcement to target priorities as well. For example, although cryptocurrencies pose a big challenge for law enforcement due to their decentralization and inherent anonymity, they have designated choke points, namely exchanges.^{359,360} They are necessary to be able to either buy coins of a cryptocurrency or, more importantly, to cash out the coins for real money.³⁶¹ Therefore, law enforcement can focus their efforts on these exchanges.

Cooperation is of high importance in combating cybercrime.³⁶² Important factors of

³⁴⁶[11], pp.52–53.

³⁴⁷[8], p.11.

³⁴⁸[11], p.53.

³⁴⁹[11], pp.52–53.

³⁵⁰[50], pp.22–23.

³⁵¹[264], p.71.

³⁵²[264], p.71.

³⁵³[265], p.81.

³⁵⁴[247], pp.533–534.

³⁵⁵[266], p.63.

³⁵⁶[267], p.387.

³⁵⁷[266], p.63.

³⁵⁸[267], p.387.

³⁵⁹[258], p.472.

³⁶⁰[257], pp.90–91.

³⁶¹[257], pp.90–91.

³⁶²[11], p.9.

international cooperation are the harmonisation of legislation, provision of operational support and resources, capacity building, knowledge exchange, and the coordination of joint actions.^{363,364} Public-private partnerships are important as well.³⁶⁵ The private sector often holds evidence of cybercrimes and cooperation can foster the reporting of crimes and the collaboration with law enforcement (for example, in the case of data breaches).³⁶⁶ The cooperation can furthermore enhance the effective take-down of criminal infrastructure, the removal of unlawful content, and the preservation of evidence.³⁶⁷ Moreover, the cooperation of law enforcement with the private sector and academia facilitates to explore and research emerging trends, technologies, and investigative approaches.³⁶⁸ As an approach to combat cybercrime and the Crime-as-a-Service economy, the strategy could be used against themselves: By division of specialization, each partner of the network develops distinct expertise and specialized skills, and makes their core competencies available to other partners of the network - *as-a-Service*.³⁶⁹

7.4 Challenges of law enforcement

Paradoxically, the successes of law enforcement causing disruptions in the cybercrime economy, also have positive consequences for cybercrime: Law enforcement is an incubator and major innovation driver for the underground economy.³⁷⁰ Law enforcement impels cybercriminals to adapt and optimize their behaviour and strategies, so as to mitigate the risk of detection and disruption in the future.³⁷¹ For example, as a result of marketplace shutdowns by law enforcement (and bolstered by exit scams), cybercriminals shift to decentralized marketplaces to avoid these kind of failures in the future.³⁷²

In general, traces of evidence in cybercrime is little to none, hence investigations are by default difficult.³⁷³ The inherent anonymous nature of the Internet allows criminals to conceal their real identity by creating a virtual identity.³⁷⁴ Law enforcement must therefore connect evidence not only with the virtual identity but must also be able to connect the virtual identity with a real identity to enable prosecution.³⁷⁵

What aggravates this even more are the various anti-forensic measures deployed by cybercriminals to hamper their attribution, conceal their real identity, and prevent law

³⁶³[260], p.7.

³⁶⁴[10], p.99.

³⁶⁵[260], p.6.

³⁶⁶[260], p.6.

³⁶⁷[260], p.6.

³⁶⁸[11], p.53.

³⁶⁹[8], p.9.

³⁷⁰[219], p.5.

³⁷¹[11], p.8.

³⁷²[11], p.53.

³⁷³[268], p.9.

³⁷⁴[265], p.71.

³⁷⁵[230], p.604.

enforcement from revealing the connection between their virtual and their real identity.³⁷⁶ Anonymisation measures, such as proxies, VPNs and anonymising networks, are part of the basic equipment of cybercriminals (cf. 7.2.1 Anonymising networks). Virtual currencies allow transactions that obfuscate the traces and, in further consequence, the connection between cybercriminals (cf. 7.2.5 Cryptocurrencies).³⁷⁷

Establishing connections between cybercriminals is also aggravated by the dispersed nature of cybercrime (also due to the impact of Crime-as-a-Service).³⁷⁸ Cybercriminals rarely know each other in real life, are likely to be distributed globally, and therefore communicate online.³⁷⁹ This makes it more difficult to draw connections, and identify and prosecute associates.³⁸⁰

As a consequence thereof, law enforcement is confronted with the challenge of establishing the physical location of a cybercriminal to determine which country has jurisdiction, which legal framework is applicable, and to avoid competing prosecution claims of countries.³⁸¹ Another aggravating factor in this regard are cloud-based services and storage, as their physical location could be located in different jurisdictions.³⁸²

Taking advantage of the challenges that law enforcement faces when multiple jurisdictions are involved is in general a strategy of cybercriminals.³⁸³ They see borders (and, consequently, different legal frameworks) as opportunities to aggravate investigations and prosecution.³⁸⁴ Therefore, cybercriminals often host their infrastructure and operate in jurisdictions where they perceive the risk of law enforcement to be lower, either due to the lack of adequate collaboration and support for other jurisdictions, or due to underdeveloped capabilities and restricted resources in these jurisdictions.^{385,386}

Although cybercriminals tend to minimize their traces, the volume of data collected by law enforcement is substantial.³⁸⁷ It is not unusual that the volume exceeds several terabyte of data in some cases.³⁸⁸ This poses a challenge for law enforcement with regards to resources and time, as it increases the difficulty of detecting relevant evidence in the vast volume of data.³⁸⁹

Furthermore, the collection of evidence is negatively impacted by the increasing use of

³⁷⁶ [50], p.69.

³⁷⁷ [11], p.9.

³⁷⁸ [50], p.22.

³⁷⁹ [50], p.22.

³⁸⁰ [50], p.22.

³⁸¹ [260], p.4.

³⁸² [260], p.5.

³⁸³ [200], p.11.

³⁸⁴ [200], p.11.

³⁸⁵ [11], p.9.

³⁸⁶ [269], pp.410–411.

³⁸⁷ [8], p.53.

³⁸⁸ [8], p.53.

³⁸⁹ [50], p.69.

encryption.³⁹⁰ This does not only apply to the communication between cybercriminals (for example, encrypted e-mails and end-to-end encryption of messenger services, cf. 7.2.3 'Communication'), which hinders the interception of communication, but also to stored data.³⁹¹ Consequently, it considerably impacts investigations due to the necessity of decryption or even leads to a loss of intelligence and evidence.³⁹²

Another major technical challenge contributes to the problems regarding attribution of cybercriminals: Carrier-grade network address translation (CGN).³⁹³ Due to the exhaustion of IPv4 addresses, IPv6 was invented.³⁹⁴ As the transition to IPv6 is only happening gradually, CGN is a temporary solution of Internet Service Providers to address the problem of IPv4 address exhaustion and to handle IPv4 and IPv6 addresses simultaneously.³⁹⁵ Part of the temporary solution is the allocation of a single IPv4 address to potentially thousands of Internet users at the same time.³⁹⁶ This significantly impairs the ability of law enforcement to associate a certain IP address with a cybercriminal, as it first requires them to investigate and determine who is behind an illicit action among all Internet users that are using the same IP address.³⁹⁷

That also implies a challenge regarding privacy and data protection, as it would require law enforcement to investigate many innocent Internet users.³⁹⁸ It is necessary to find the right balance between the capabilities of law enforcement, to allow them to intervene when and where necessary, and the citizen's rights for protection of their privacy and data.^{399,400} A prominent example is encryption: While legitimate to use and useful for businesses and citizens to protect their data, it poses a major challenge for law enforcement.^{401,402}

Another major challenge for law enforcement is the speed, evolution and growth of cybercrime in both volume and practices.⁴⁰³ Keeping pace is therefore often difficult for law enforcement.⁴⁰⁴ It requires them to remain current and to be adaptive and agile with regards to new developments, while respecting the admissibility of law enforcement methods, which are often hampered by slow and bureaucratic processes and programmes.^{405,406} Moreover, this is also challenging regarding law enforcement

³⁹⁰ [8], p.46.

³⁹¹ [260], p.3.

³⁹² [260], pp.3–4.

³⁹³ [8], p.57.

³⁹⁴ [50], p.56.

³⁹⁵ [8], p.57.

³⁹⁶ [50], pp.56–57.

³⁹⁷ [8], p.58.

³⁹⁸ [260], p.3.

³⁹⁹ [50], p.72.

⁴⁰⁰ [11], p.65.

⁴⁰¹ [270], pp.8–9.

⁴⁰² [8], p.46.

⁴⁰³ [10], pp.98–100.

⁴⁰⁴ [260], p.7.

⁴⁰⁵ [269], p.429.

⁴⁰⁶ [8], p.9.

resources, making it necessary to set priorities regarding actions and initiatives.⁴⁰⁷

⁴⁰⁷[50], p.71.

Investigative research in the Crime-as-a-Service economy

8.1 Objectives and procedure

The general objective of this chapter is to find out more about the facilitating role of Crime-as-a-Service with regard to e-commerce fraud. To commit e-commerce fraud, fraudsters must be prepared for all three processes of an e-commerce transaction: In the agreement process, identity data are required to create the impression of a legitimate customer. In the payment process, valid payment data must be on-hand to be able to continue the transaction. Finally, in the delivery process, fraudsters must find a way to be able to receive the fraudulently obtained goods in order to monetize them.

Therefore, the objectives for the investigative research are related to the as-a-Service business models as explained in the previous chapter: Data-as-a-Service and Reshipping-as-a-Service.

Regarding data, depending on the used means of payment, fraudsters need payment data, either stand-alone or in combination with identity data of the legitimate account holders. The latter is of more value for fraudsters, as it increases the likelihood of a successful fraud attempt. The payment data of relevance are credit and debit card data and credential data for e-wallets: these are not only the most common payment methods (cf. 2.5 'Online payment') but also pose a considerable risk regarding e-commerce fraud (cf. 3.3.2 'Evaluation of online payment methods').

Regarding the delivery of fraudulently obtained goods, it is of interest to find out more about ways to receive the goods and offers of Reshipping-as-a-Service providers.

Moreover, of relevance is also information that helps fraudsters learn and refine their strategies. Therefore, it is also of interest to find out more about the knowledge that is available for fraudsters in the cybercrime community, such as instructions and tutorials.

It is also common that cybercriminals share or trade exploits with each other. Exploits in the context of e-commerce fraud are vulnerabilities within a merchant's e-commerce process that are ferreted out by cybercriminals, allowing them to exploit the identified vulnerability to accomplish an e-commerce fraud attempt.¹ Therefore, this type of exploits is among the objectives as well.

To summarize it, the objectives for the investigate research are as follows:

- Investigate ways to acquire the following data required to commit e-commerce fraud:
 - Credit and debit card data
 - E-wallet credentials
- Investigate ways to receive fraudulently obtained goods:
 - Information about how to receive fraudulently obtained goods
 - Offers of Reshipping-as-a-Service providers
- Investigate ways to gather relevant information about e-commerce fraud:
 - Exploits
 - Information in general about how to commit e-commerce fraud

It is beyond dispute that the service-oriented cybercrime community offers the required data, information, and services listed in the objectives.² Thus, the focus of the investigative research is not whether these required commodities are available in the cybercrime community, but how available they are for e-commerce fraud novices, i.e. unskilled fraudsters without previous e-commerce fraud experience and non-existent experience and reputation in the cybercrime community. As Crime-as-a-Service is accused of diminishing the entry barrier for entry-level cybercriminals, the expected outcome of this investigative research is to either confirm or disconfirm this allegation with regard to e-commerce fraud.^{3,4}

The investigative research is carried out in the Darknet, namely in the most heavily used anonymising network for illicit activities: the Tor network.^{5,6}

The proceeding requires an exploratory approach due to the nature of the Darknet. For clarification, it must be distinguished from the *Surface Web*, the *Deep Web* and the *Darknet*.⁷

¹[8], p.29.

²[254], pp.3–4.

³[11], p.7.

⁴[254], p.29.

⁵[50], p.55.

⁶[237], pp.15–16.

⁷[52], p.23.

The *Surface Web* (also referred to as World Wide Web) is the part of the Internet that is publicly available to anyone.^{8,9} It consists of any web page that can be indexed and found by a search engine.^{10,11} In contrast to the Surface Web, the *Deep Web* consists of any web page that can't be indexed and found by a search engine.^{12,13} This comprises, among others, dynamic web pages (i.e. web pages where the content adapts dynamically, for example depending on user input), web pages that require some form of authentication to access them (for example, password-protected forums), or web pages that are deliberately designed not to be indexed by search engines (and are therefore only accessible via a direct link).^{14,15} It is estimated that considerably more than 90% of the Internet belongs to the Deep Web.^{16,17} Part of the Deep Web is the *Darknet* (also sometimes referred to as *Dark Web*), i.e. anonymising networks that can only be accessed using specialized software and are intentionally hidden to the public.^{18,19} It only accounts for a fraction of the Deep Web with an estimation of about 0.01%.²⁰ A popular way to depict the scale of the Surface Web, the Deep Web and the Darknet is to use an iceberg as an illustration, as shown in figure 8.1.

There are two ways to start navigating through the Darknet: Firstly, by using search engines which are specialized in and designed for indexing and searching hidden services in the Darknet.^{22,23} Secondly, by making use of link directories, which provide lists of links to hidden services.^{24,25} A prominent example among these directories is the so-called *Hidden Wiki*, which provides a considerable number of links listed by category.²⁶

The investigative research is restricted to content that is freely available. This also includes areas that require a registration to be able to access the content. Not included are areas that require a payment to be able to receive or get access to information in order to not violate any laws and commit a punishable crime.

⁸[271].

⁹[272], p.3.

¹⁰[271].

¹¹[272], p.3.

¹²[272], p.4.

¹³[273].

¹⁴[272], p.4.

¹⁵[273].

¹⁶[274].

¹⁷[275].

¹⁸[272], p.4.

¹⁹[271].

²⁰[275].

²¹Modified from [273].

²²[276].

²³[277].

²⁴[278].

²⁵[276].

²⁶[279].

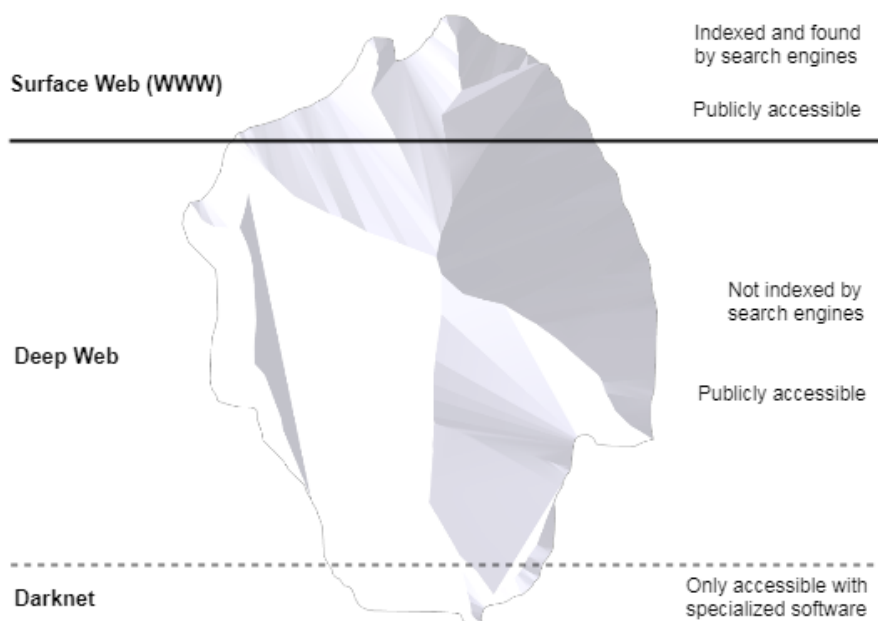


Figure 8.1: Schematic illustration of the scale of the Surface Web, the Deep Web and the Darknet²¹

8.2 Prerequisites and preparation

The Darknet is a place known to be frequented by cybercriminals of all sorts, such as hackers and scammers. Therefore, focusing on preserving privacy, anonymity, and security is imperative in the Darknet.^{27,28} It is also recommended to create a fake identity (which, naturally, should have no connection whatsoever to the real identity) or even multiple fake identities for different purposes.^{29,30}

The most widely used software to access the Tor network is the *Tor Browser*^{31,32} It is an open source and based on Mozilla's Firefox browser with enhanced encryption, privacy, and security settings.^{33,34} This also comprises restrictions and avoidance of various plugins and technologies, such as Java, JavaScript and Flash.³⁵

A practical solution to access the Darknet is Tails³⁶ (abbreviation for *The Amnesic*

²⁷[280].

²⁸[281].

²⁹[278].

³⁰[282].

³¹Available at <https://www.torproject.org/projects/torbrowser.html.en>

³²[283].

³³[284].

³⁴[281].

³⁵[284].

³⁶Available at <https://tails.boum.org/index.en.html>

Incognito Live System), which “aims at preserving your privacy and anonymity, and helps you to: use the Internet anonymously and circumvent censorship; all connections to the Internet are forced to go through the Tor network; leave no trace on the computer you are using unless you ask it explicitly; use state-of-the-art cryptographic tools to encrypt your files, emails and instant messaging”³⁷. Tails is a Debian-based live operating system, i.e., it can be used from a removable media (USB stick or DVD), which is reset every time the system starts.³⁸ It comprises pre-installed and pre-configured applications with consideration for security, such as the Tor browser, clients for e-mail and messaging, and cryptographic tools, among others.^{39,40} Besides the benefit of having a pre-configured, ready to start environment focused on security to access the Darknet, a further advantage is that it is a standalone system and, thus, not tied directly to the personal device of a user.⁴¹

8.3 Investigation

As mentioned previously, searching for resources on the Darknet differs from searching on the Surface Web. Therefore, the explorative approach to find the sought resources is defined as illustrated in figure 8.2: Initially, a search on the Surface Web is conducted for links to Darknet directories and Darknet search engines; the directories are also used to discover further search engines. Together they form the starting basis for discovering hidden services in the Darknet, namely forums, marketplaces, shops, and other hidden services (that don’t fit in the other categories). References (i.e. links) that can be found there are used to further extend the search results of sought services.

All hidden services mentioned throughout this chapter are listed with the respective .onion address in Appendix B ‘Investigation in the Darknet’. Moreover, since the access to the Darknet is restricted for the public, screenshots are added as well to document the investigation.

The introduced explorative approach resulted in a starting basis consisting of the Darknet search engines *Candle, not Evil*, and *Torch*, and the directories *Fresh Onions*, *Hidden Wiki*, *The 2017 Verified Hidden Wiki*, *The Hidden Wiki*, *The Uncensored Hidden Wiki*, and *UnderDir*. On that basis, the hidden services with regards to e-commerce fraud described below were discovered.

8.3.1 Forums

As described in the previous chapter, forums serve multiple functions for cybercriminals. The forums discovered during the investigation were either completely focused on carding

³⁷[285].

³⁸[286].

³⁹[286].

⁴⁰[287].

⁴¹[281].

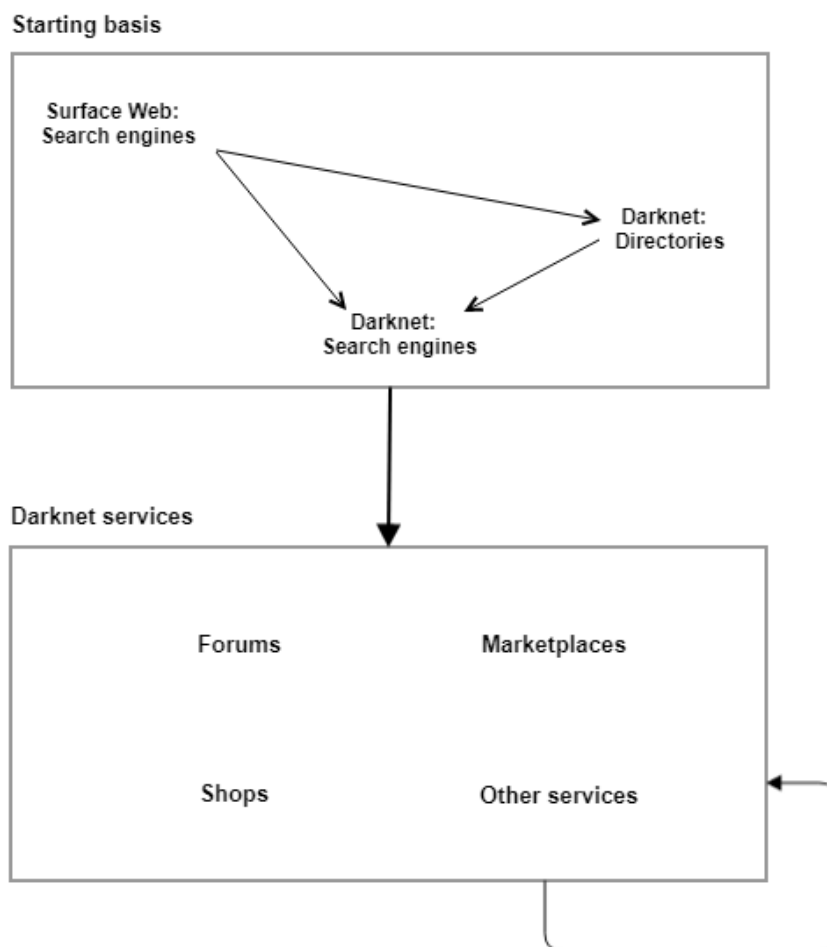


Figure 8.2: Explorative approach for discovering hidden services in the Darknet

and topics related to it (such as security measures), or with a broad focus on cybercrime topics (including carding).

Examples for forums dedicated to or mainly concerned with carding are *CLUB2CRD* and *ShadowCrew*. They are accessible free of charge (some forums activate new accounts instantly, while others need a manual activation by one of their administrators), while other forums specialized in carding, such as *GGMCCLOUD1*, *Kickass* and *Omerta*, are only accessible when a membership fee is paid in advance.

A special case among the investigated forums is *Tor Carding Forum v3*, as the hidden service is only used to refer to their forum on the Surface Web. *SKY-FRAUD.RU* is accessible via both the Darknet and the Surface Web; the focus is on carding, hacking and security. *The Onion Forum* also has a broader focus and is concerned with cybercrime topics in general, including carding and related aspects.

Excluding forums with a membership fee, only a registration is required to be able to access the content of the forums and interact with other members. The emphasis varies among these forums: *ShadowCrew* is very community-driven, where members provide a multitude of tutorials, look for accomplices and help each other. *CLUB2CRD* is mainly used by members advertising illicit services, which also applies to *SKY-FRAUD.RU*.

The topics and advertised services in the forums are indeed able to cover every part of e-commerce fraud: It is common for these forums to have an area for trading or advertising illicit services. This enables forum users to find sought commodities required to commit e-commerce fraud, such as credit card data, exploits and guides for merchants systems, and mail drops. Moreover, the members support each other by answering questions, giving guidance and recommendations, and providing tutorials. Therefore, forums are a suitable way for beginners to start an e-commerce fraud career.

8.3.2 Marketplaces

Cybercrime marketplaces are known to be a place for trading any kind of illicit goods and services (cf. 7.2.4 'Marketplaces'). Currently, the five biggest marketplaces in the Darknet are *Dream Market*, *Silk Road 3*, *The Trade Route*, *Valhalla*, and *Tochka*.⁴²

All of these marketplaces can be found easily (the respective .onion links can be even found on the Surface Web). Some of them allow users to browse the offers without registration, while others are restricted to registered users. However, registering for an account is open for everyone at each of these marketplaces and often only require a username, a password and the input of a so-called CAPTCHA⁴³ code (to ensure the account is registered by a human and not in an automatized way).

The investigation of the marketplaces and their offers shows that the majority of offered products are related to narcotics. However, on each of these marketplaces fraud-related offers are traded as well. In fact, with regard to e-commerce fraud, anything necessary to commit e-commerce fraud can be acquired.

Credit cards are traded in various quantities, ranging from a single credit card to a bulk of cards, with specification of the region (such as Europe or the United States) and varying extents: While some offers only comprise the data that can be found on a physical credit card (i.e. credit card number and card security code), others cover the data of the legitimate account holder as well (usually advertised as "fullz").

PayPal accounts are traded as well, also in varying quantities and to varying extents: Some offers comprise PayPal accounts with a preloaded balance, identity information about the legitimate account holder, or PayPal accounts with connected credit cards or bank accounts.

The marketplaces not only provide the necessary commodities to commit e-commerce fraud (such as credit card data or e-wallet credentials), but they are also full of guides

⁴²[288].

⁴³Acronym for *Completely Automated Public Turing test to tell Computers and Humans Apart*

and tutorials that teach the necessary skills required by fraudsters. In fact, for each element of e-commerce fraud the required knowledge can be acquired: ranging from how carding works in general, how to use credit cards or e-wallet credentials without the risk of “burning” (i.e. blocking) it, to instructions explaining how to target specific merchants (such as Amazon, ebay, Dell, among others) and successfully committing fraud.

Although there are no direct offers for reshipping services, there are offers for guides and tutorials about the required knowledge on drops and how to set up drop points to receive fraudulently obtained goods. Additionally, directories containing mail drops can be purchased.

Marketplaces basically offer anything that is required to get the skills and commodities necessary to successfully commit e-commerce fraud. Due to the easy access of these markets, the reputation system (which mitigates the risk of falling victim of a bogus vendor), and the competition among vendors resulting in low prices, marketplaces are indeed a helpful source for fraudsters, especially for beginners.

8.3.3 Shops

Another way to acquire illicit commodities are shops. These services are specialized in certain products (such as credit card data, physical credit cards, forged documents, or PayPal accounts), which can be found easily via Darknet search engines (for example, by searching for "carding shop"). Many of them are also listed in directories. Moreover, it is not uncommon to stumble upon banner adverts for these shops, as they are advertised heavily in the Darknet.

Some examples for such shops with regards to e-commerce fraud are *7YearsinTibet* (credit cards, PayPal accounts), *Cash Machine* (credit cards, PayPal accounts, bank accounts), *MrRobotShop* (credit cards, PayPal accounts, bank accounts), *netAuth* (credit cards, PayPal accounts), *Reborn Market* (credit cards, PayPal accounts, bank accounts, accounts for Amazon and ebay), *TGSS Carding* (credit cards, PayPal accounts, gift cards), and *VendorPro* (PayPal accounts, bank accounts).

The operators of these shops strive to purport running a legitimate, reliable service that emphasizes customer service: It is common that these shops pledge to refund or replace corrupt products (for example, if a credit card is blocked), and to provide support within a few hours.

Basically, all of the investigated shops have the same procedure in the form of a (semi-)automatic process: A customer can select the desired products; to complete the order process, an e-mail address must be entered. After that, an order confirmation is presented to the customer with a payment request. Payments must usually be paid with Bitcoin; thus, customers are requested to pay their order by sending the payment amount to the displayed Bitcoin address. Upon receiving the payment, the vendor assures to mail the ordered products or further instructions to the specified e-mail address.

However, while it is fairly easy to verify the legitimacy of a shop on the Surface Web, the anonymity and, thus, lack of options to validate a service in the Darknet result in an odd situation: Shops are a popular scam tactic to trick unknowing users to pay for products they will never receive. While some of the directories, such as *The Uncensored Hidden Wiki*, use a rating system to point out scams (where almost all shops are marked as scams), other directories don't provide this information. As directories are often the starting point for beginners in the Darknet, the suspicion is that links to scam shops are listed intentionally.

In communities, such as the *Hidden Answers*, users ask regularly about the legitimacy of shops, or share their negative experience after having fallen for a scam shop. The prevailing opinion is that shops should be avoided; instead, marketplaces are recommended to acquire products, as their rating and reputation system mitigates the scam risk.

8.3.4 Other hidden services

The service *Hidden Answers* is a Q&A community, where people can post any kind of question (anonymously or using a nickname), and other Darknet users can answer it. With regards to e-commerce fraud, it is often used to get advice or recommendations, such as where to find a reliable vendor to acquire illicit commodities (for example, credit card data), or if a certain service (such as a marketplace or shop) is a scam or legit.

There are also course providers on the Darknet that teach carding skills required to be able to commit e-commerce fraud, such as *Carders University* and *KINDLES - Carding lessons*. *KINDLES*, which also receives positive feedback and recommendations from users of *Hidden Answers*, offers three courses: carding lessons are offered for 225 US\$, PayPal lessons for 300 US\$, and full carding lessons (which teaches extensive skills for carding and PayPal) for 800 US\$. *Carders University* offers multiple courses, where one course is concerned with carding for 600 US\$; another course is concerned with PayPal for 420 US\$.

8.4 Summary

It is safe to say that the Darknet, or to be more exact, Crime-as-a-Service, offers anything that is necessary to commit e-commerce fraud. Required data, i.e. credit card data and e-wallet credentials, can be purchased, as well as information about how to commit fraud at specific merchants. The same applies to services that support committing e-commerce fraud (such as services that enable the user to use an IP address that appears in the local area near the legitimate account holder to circumvent fraud detection systems, or to check the validity of credit cards). Moreover, the offered guides, tutorials and courses allow interested users to establish and improve their illicit skills. Also the cybercrime communities can play an important role regarding e-commerce fraud.

However, the investigation has clearly shown that the Darknet is not a safe place - for beginners. While at first glance it seems to be a place where literally everything can

be purchased, from hitmen for hire (which advertise their services with eye-catching banner adverts), and drugs, to e-commerce fraud commodities, chances are high that the advertised services are a scam. Therefore, it can be assumed that a lot of the business models in the Darknet are only based on (and only work due to) the unawareness of (most likely) new users. Hence, the Darknet is not a place where possibilities to earn easy money are waiting, at least not for beginners. Nevertheless, by spending time and acquiring skills and experience, users are indeed able to advance into the depths of the Darknet, obtain sought commodities and services, and expand their skills.

It can therefore be assumed that the easier a product or service can be found and acquired, the more likely the chance that it is a scam, and vice versa: With more experience and awareness of the inherent scam risk, as well as connections and reputation in communities, sought commodities can be found and purchased without a hassle. Mechanisms to counteract the lack of ways to validate the legitimacy of a provider, such as the rating and reputation systems at marketplaces, can lower the risk and establish trust. It is also common to use an escrow service for purchases, so that the money of a buyer is only transferred to the vendor once the buyer has received the goods or service.

A lot of information (for example, about how to commit e-commerce fraud, or how to establish a mail drop) is freely available. However, since Crime-as-a-Service is business model-oriented, and, thus, focused on monetizing service offerings, it is necessary to invest some money to receive all information, commodities and services required to successfully commit e-commerce fraud. For payments, the undisputed number one currency in the Darknet is Bitcoin. Therefore, a lot of hidden services exist that are concerned with Bitcoin transactions, such as mixers to confuse the trail of a transaction.

It can also be observed that safety awareness and paranoia among users of the Darknet are omnipresent. It is common that users remind other users who are interested in illicit things to be mindful of the measures to stay anonymous and not get caught by law enforcement. The paranoia is fueled by the fact that it is possible to stumble upon hidden services where visitors are greeted with the information that the hidden service has been seized by law enforcement. The National Police and Public Prosecution Service of the Netherlands even runs their own hidden service where they list the nicknames of Darknet users that were actively trading at the seized *Hansa Market* with the message: "*The Police and Judicial Authorities of the Netherlands are active in the real world, but also in all corners of the Internet. We trace people who are active at Dark Markets and offer illicit goods or services. Are you one of them? Then you have our attention.*".

Also the competition in the Darknet and the consequences thereof are remarkable. The investigation was conducted over several days, and there was hardly any point in time where all of the investigated marketplaces were available simultaneously. It is common that marketplaces are the target of DDoS attacks⁴⁴, and are, consequently, not available

⁴⁴DDoS, abbreviation for Distributed Denial-of-Service, is the attack of infrastructure (such as servers) by consuming and exhausting available resources with the intention of rendering a service (for example, a marketplace) unavailable. [289], pp.40-41.

for a certain time. Among the reasons for DDoS attacks is competition among marketplace providers with the intention to damage other competing marketplaces.⁴⁵

Moreover, due to the inherent anonymity, and, therefore, the lack of measures to verify the validity and reliability of a service, it can also be exploited by competitors. While the cybercrime community is a valuable source with regards to the validity of a service (if it is legit or a scam), competitors can make use of this mechanism: By proclaiming that a service is a scam, the reputation of the service can be damaged, thus resulting in a loss of users and sales.

In summary, it can be said that Crime-as-a-Service provides anything necessary to commit e-commerce fraud. Although the Darknet holds some traps for novices, it is safe to say that Crime-as-a-Service diminishes the entry barrier for beginners, allowing them to become professional fraudsters, or at least equip them with anything necessary to commit e-commerce fraud in a professional way.

⁴⁵[290].

Conclusion

E-commerce fraud is essentially the abusive use and exploitation of a payment method's and delivery service's weak spots with the intention of monetizing payment information (cf. 3 'E-commerce fraud'). Regarding payment methods, several are safe to use and provide a sufficient level of security for legitimate account holders, while other payment methods can easily be used in illicit ways. In particular, payment methods that can be stolen easily and only require a basic set of data to complete a payment without a layer of security, such as a password, are prone to e-commerce fraud, namely credit cards and payment after delivery. E-wallets also pose a certain amount of risk if the credentials get into the wrong hands. In addition, delivery services are exploited in ways that enable fraudsters to receive the fraudulently obtained goods without the risk of revealing their real identities, to avoid prosecution, and to circumvent delivery limitations.

Cases of e-commerce fraud often show certain characteristics; however, the challenge is that only indicators exist to determine whether or not a transaction is fraudulent. Examples include, among others, the unusual behaviour of a buyer, such as multiple attempts to pay with different credit cards, as well as saliences in order details, such as over-average orders or atypical product combinations. Nonetheless, it is often not possible to be certain about the legitimacy of a transaction. For example, fraudsters typically use the legitimate account holder's payment details but enter a different shipping address when making illicit orders. While it could be an indicator for fraud, it could also be a perfectly legitimate transaction, i.e., a shopper ordering something for a third party, such as a gift. A particular challenge regarding e-commerce fraud is related to first-time buyers, as there is no purchase history that could prove the buyers' legitimacy.

Prevention of e-commerce fraud is concerned with establishing an environment where e-commerce fraud is avoided before it can take place (cf. 4 'Preventing e-commerce fraud'). An important factor in this regard is the analysis of past fraudulent transactions, as it does not only assist in revealing weak spots that are exploited by fraudsters, it also derives patterns that can help reveal illicit transactions. Consequently, based on knowledge

acquired from the past, adaptations can be made to prevent e-commerce fraud in the future. As e-commerce fraud is, in fact, always based on identity fraud, identity verification is one of the main issues. Various approaches exist to tackle this problem, ranging from data verification and identity verification measures, such as ID checks, to the usage of trusted virtual identities. Payment methods are evolving as well, and due to the need for more security, additional security measures have been established, for example, '3D Secure' assist in making online payments with credit cards more secure. A more radical way to prevent the exploitation of a payment method's weak spots is to restrict the use of them, either generally (i.e. not providing a certain payment method that is susceptible to fraud) or partially (i.e. not allowing certain customers, such as first-time buyers, to use certain payment methods). Prevention measures can also involve delivery services: either by making use of provided security measures, such as delivery tracking, or by restricting certain services, such as parcel forwarding. Although effective measures to prevent e-commerce fraud are existent, the bigger challenge is finding the right balance between prevention measures and customer satisfaction. According to all interviewed experts, customers expect easy, fast, and frictionless processes; by not meeting customer expectations, the risk of customer loss is to be expected, thus hampering prevention measures.

E-commerce fraud detection measures are concerned with revealing fraudulent transactions as soon as possible, at best immediately, or at the very least before a transaction has progressed so far that a loss is inevitable (cf. 5 'Detecting e-commerce fraud'). The task of fraud detection can be reduced to a deceptively simple task: deciding whether a transaction is fraudulent or not. This is, however, a very complex task, and many factors have to be considered. Among the challenges are the limited time span that is available for fraud detection, the large amount of data and unbalanced composition of data (mostly legitimate transactions versus fewer fraudulent transactions), incomplete information (cases of fraud are often revealed after it is already too late) and false alarms. False alarms can cause costs in two respects: Losses occur not only if fraud attempts are successful, but also when legitimate transactions are wrongly classified as fraudulent, which, in the worst case scenario, can lead to a loss of customers. Different approaches for fraud detection exist, where each approach has its own advantages and downsides. For instance, manual reviews, while usually accurate (depending on the reviewers) and not based on sophisticated systems, have problems regarding scalability. Furthermore, information providers are used to collate and, thus, verify the data of a transaction; the accuracy of these systems is dependent on the quality of the underlying data and is often limited, among other reasons, due to data privacy issues. Systems based on data analysis exist in various forms: (1) Rule-based systems, where the accuracy is directly related to the quality of the rules, and continual updates are required, (2) supervised classification, where the classification of transactions is based on the knowledge of past transactions, and (3) unsupervised anomaly detection, where unusual salience is detected in a transaction originating from a previously determined baseline. As each system has its own set of disadvantages, the combination of various fraud detection systems makes it possible to benefit from all of the desired advantages, reducing the respective downsides.

With that being said, the main issue in this regard is the underlying costs: As mentioned by one expert, it would be theoretically possible to dramatically eliminate fraud, but because each system causes costs and fraud detection systems are ultimately supposed to be an economic solution, the total elimination of fraud isn't feasible.

The analysis of the legal situation regarding e-commerce fraud (cf. 6 'Legal aspects and prosecution of e-commerce fraud') demonstrates that existing laws would be sufficient to prosecute e-commerce fraud and related activities. However, prosecution is, in most cases, rather difficult due to the challenges faced when investigating offenders, as well as the inherent cross-border character of e-commerce fraud that aggravates investigations even more. Transnational endeavours are in place, and they are indeed a basic element in the fight against e-commerce fraud; however, they are outdated and commonly lag behind the fast-evolving cybercrime community. Additionally, rules alone are simply not enough. Organizations, such as Europol or Interpol, and international cooperation between these organizations and countries are required to effectively take measures against e-commerce fraud. If there is a lack of these structures and cooperation, which is true in many cases, e-commerce fraud will pose a serious challenge for law enforcement.

The Crime-as-a-Service economy and its service-oriented business model, based on the specialization of criminals and the division of labour, facilitates and contributes to the increase in e-commerce fraud (cf. 7 'Crime-as-a-Service'). Amateur criminals are able to commit crimes, such as e-commerce fraud, and operate on a level beyond their capabilities due to the reliance on highly-skilled cybercriminals who strive to monetize their illicit services and goods; thus, the entry barrier for cybercriminals who intend to commit e-commerce fraud is lowered. Of particular importance is Data-as-a-Service, which provides criminals with the data required to commit e-commerce fraud, such as credit card and identity data, and Reshipping-as-a-Service, used by criminals to receive their fraudulently purchased goods. For law enforcement, the thriving cybercrime community is hard to tackle, and only lasting counter-measures that cause disruptions, either temporarily or permanently, prove to be effective. Again, cooperation between organizations and countries are required to effectively combat the Crime-as-a-Service economy.

The future regarding e-commerce fraud does not look so bright, as there appears to be no foreseeable end in sight. The ever-increasing volume of e-commerce transactions as well as the aforementioned reasons play a fundamental part regarding this outlook. Furthermore, fraudsters will continue committing fraud, bolstered by the Crime-as-a-Service economy, as long as it is profitable for them. Prevention and detection measures are aggravated due to the need to be customer-oriented, efficient, and economical. Moreover, law enforcement is often hampered by the inherent cross-border character of e-commerce fraud, and, as mentioned by one expert, criminals are not only one, but always two steps ahead.

Nevertheless, the fight against e-commerce fraud is not hopeless, as there are ways for merchants to gear up for and take measures to protect themselves from fraudsters targeting e-commerce transactions. Systems to detect fraudulent transactions are continuously being developed and becoming more and more effective. Since the majority of e-commerce

fraud is committed with the illegitimate use of credit cards, the invention of 3D Secure is of great significance. As the rollout of this security measure is progressing, it will contribute to making the lives of fraudsters, targeting e-commerce transactions, more difficult. As mentioned by one experts, the extent to which the weaknesses of e-commerce transactions can be exploited will continue to increase until the negative effects for involved parties are finally considered unacceptable. Thereupon, measures are invented to respond to the threat. This was the case with credit cards and 3D secure, and it is likely to be the case with other weak spots, such as payment after delivery, upon reaching a certain level of negative effects. Moreover, as stated by the experts, in the hope of aggravating e-commerce fraud, it is important to raise awareness and educate society about the security measures of payment methods, about what shoppers should bear in mind when shopping online, and about the various schemes of fraudsters.

The bad news is, proven by past experiences, that fraudsters will not surrender and will either find new ways to commit e-commerce fraud, or shift to another mode of fraud.¹ As long as there is an anticipated low risk and effort, and expected high profits, e-commerce fraud will continue to remain attractive for fraudsters.

Two main limitations were perceived when writing this thesis: Firstly, the delivery process of an e-commerce transaction is currently neglected by scientific research. Although the delivery plays a fundamental part of e-commerce fraud, the existing scientific literature regarding this topic is inadequate. Secondly, in scientific literature, it is common for e-commerce fraud not to be examined as a whole; instead only parts of it are taken into consideration. Popular topics within the scientific scope, such as detection methods and the illicit usage of credit cards, receive a lot of attention, while other topics are less researched. Furthermore, the analysis of e-commerce fraud as a whole, where all three phases of an e-commerce transaction (agreement, payment, delivery) are considered, has also been neglected. Conclusively, in order to better understand e-commerce fraud as a whole, to be able to identify weak spots, and to react accordingly and effectively, both aforementioned limitations, with particular focus on the latter, must be given their due attention in the future.

¹[60], p.258.

Expert interviews

A.1 General

Between June and November, interviews with five e-commerce fraud experts were conducted. The interviewees are from three areas: Firstly, two experts are from law enforcement agencies who are involved with investigations and actions against criminals committing e-commerce fraud. Secondly, one expert is responsible for the risk department of a payment provider, and, thus, concerned with e-commerce fraud in daily business. Thirdly, two experts are from merchants who are confronted with e-commerce fraud and measures against it in their routine business.

In general, expert interviews are used, among other reasons, for exploration and orientation in a topic and to collect practical information and insights about behaviors, experiences, practices, beliefs, or opinions.^{1,2}

For the thesis at hand, the purpose of the interviews was to get practical insights and information from experts about the current situation and the impact of e-commerce fraud, measures against it, and the prospects regarding e-commerce fraud. Moreover, the content of the interviews was not only used to extend and help evaluate the knowledge gained from the literature analysis, but also to obtain new leads for further research.

The interviews were either conducted in person or via telephone and took, on average, approximately one hour to complete. Notes were taken during the interviews, and the content was subsequently summarised. To ensure that only correct information and no sensitive or internal knowledge will be published, each interviewee received the summary afterwards to approve its content. Due to the sensitive topics discussed, the experts will remain anonymous to ensure that conclusions are not drawn about their identities or, in the case of the payment provider and the merchant experts, their employers.

¹[291], pp.228–230.

²[292], p.24.

Prior to the interview, each interviewee was informed about the duration and format of the interview. Additionally, each interviewee received an interview guide to become familiar with the expected content of the interview. Depending on the interviewee's area of expertise, the interview guides were slightly adapted accordingly. Other practical reasons for using an interview guide were that it aids in covering all planned topics, makes sure that all required information is gathered, and helps prevent digression.

Due to the limited sample size, the content of the interviews is not generally applicable, but rather reflects the opinions and views of the interviewees.

A.2 Interviews with investigators

A.2.1 Focus areas of the interviews

- **General**
 - Extent of e-commerce fraud
 - Affected branches and products
 - Facilitating factors
 - Background
- **Countermeasures**
 - Measures
 - Challenges
- **Investigations**
 - Means
 - Challenges
 - Enhancements
- **Crime-as-a-Service**
 - Impact on e-commerce fraud
 - Measures

A.2.2 Investigator of Europol

Agency	Europol
Department	EC3 - European Cybercrime Center, Strategy
Date & Time	26.06.2017, 14:00-15:00

General

E-commerce fraud will continue to increase in the future. This is due to the generally increasing volume of e-commerce, as well as the growing number of Internet users and companies doing business and offering their products online. The higher volume will naturally lead to an increase of cases of e-commerce fraud. Additionally, new services and ways to do business online are continuously established, such as new means of payment, which provide fraudsters new ways to attack.

Europol is mainly concerned with crimes committed by groups, and is only involved if the crimes are cross-border. They coordinate global actions, targeting organized crime.

From their experience, there are no specific product types that are especially targeted by fraudsters. It depends more on the platforms that are prone to fraud attempts, and the products they are offering.

There are numerous factors facilitating e-commerce fraud:

Investigations are generally complex. It is easy to conceal one's real identity and location on the Internet, thus providing anonymity. It is also a question of priority of law enforcement, and a consideration of the cost-benefit ratio. Cases of e-commerce fraud are almost always cross-border, which adds to the complexity of the investigations. Therefore, the role of platforms such as Europol is important, as they coordinate global actions against organized crime.

Crime-as-a-Service has a big impact on e-commerce fraud, as it provides tools and services which facilitate committing cybercrimes.

Moreover, the industry is not using and implementing measures that are able to prevent fraud to a sufficient extent.

The main driving factor of e-commerce fraud are economic considerations - where can money be made with which effort. There is also an asymmetry regarding the risk and effort in contrast to the return potential for fraudsters: while the risk and effort is low in the case of e-commerce fraud, the return potential is high. This is definitely an incentive for fraudsters to commit e-commerce fraud.

There are no specific countries that are especially targeted by fraudsters; it depends more on the general rate of Internet penetration. Cybercrime, in general, has a strong relation to Russian-speaking regions.

Countermeasures

In order to be able to pro-actively fight fraud, it is essential that the collaboration between the police, industry and research be strengthened. This enables to define measures together, and encourage the exchange of information and intelligence. In addition, the political authorities are responsible for providing money for the required research.

The industry must strive to implement measures for more secure systems. Again, the political authorities can encourage this by providing the legal framework and incentives to strengthen the security.

Support from the police is important as well. They not only cause an “interruption of operation”, but also provide a more sustainable solution, as they can trace the criminals behind an offence and bring them to justice.

In general, to prevent cases of e-commerce fraud it is necessary to raise awareness regarding the risks of e-commerce fraud and the benefit of security measures, which is also an important strategy of Europol.

There is no way to completely eliminate e-commerce fraud, as there is also no way to completely eliminate crime. E-commerce provides too many ways to commit fraud with a tempting amount of monetary incentives for fraudsters.

Therefore, the objective is not to eliminate e-commerce fraud, but to minimize it. A certain amount of fraud is usually accepted, and regarded as common risk that is part of the business. As long as it is under a certain threshold, it is considered tolerable; measures to lower it further would not be cost-effective or economical.

It is necessary to find a balance with regard to security measures in order to keep e-commerce usable and attractive to customers. New measures would also require the coordination and collaboration of the market to prevent customer churn. If only one merchant would introduce measures to strengthen the security, which negatively impact the customer convenience, chances are high that a customer would switch to another merchant. This is, for example, a big problem with airlines. A rethinking would be required, to not see each other as competitors in this regard, but to work together on solutions to reduce e-commerce fraud.

Also customer awareness must be increased regarding measures to enhance the security of e-commerce transactions. The protection of customers, as is the case with credit or debit cards, also has an impact on customers and their understanding of security measures. They are protected, and are therefore often careless with their means of payment. It is important to build customer awareness and foster the acceptance of security measures, which would be considered a positive approach. The alternative would be to shift the responsibility to customers, forcing them to be more careful, which could be seen as a more negative approach to accomplish the desired effect.

Investigations

Investigations are done online and offline as well, depending on the possibilities and objectives. Various methods are combined, and the most promising combination is chosen, depending on the respective case and the complexity of the investigations.

The Internet itself already provides a high grade of anonymity and ways to increase it even more. For example, end-to-end encryption is becoming the standard, and technologies such as Tor add to this as well. Therefore, criminals already have a good basis for covering their tracks and hiding their true identity and location.

Next to anonymity, another challenge is the inherent cross-border character. This makes tracing criminals more difficult, as usable data is often hard to locate. Additionally, it is necessary to not only find out where usable data is located, but it must be requested and provided by a country as well. Often, the data is encrypted and not available in an open format. While the co-operation between some countries works very well (for example, within the EU), some countries are less co-operative, and are not or less willing to provide data or extradite suspects.

Crime-as-a-Service is based on the division of labour, the specialization of roles and groups, and value chains between them. Therefore, it is often difficult to determine the structures and actors behind e-commerce fraud offences.

Virtual currencies (such as Bitcoin) add to this as well, because tracing the cash flow is aggravated.

In addition, technical progress increases the difficulty. Cloud computing, for example, makes it more difficult to locate data, and often raises the question of legal competences. Carrier-grade NAT, invented as a workaround for the exhaustion of IPv4 addresses, allowing multiple users to surf on the Internet with the same IP address, makes it more difficult to track down the person behind a certain IP address.

To improve investigations, Europol identified several points: strengthening legal frameworks and co-operation among countries as well as public-private partnerships with industry and research, establishing a framework for online investigations in underground networks, solutions for the technical challenges, and training law enforcement and law enforcement authorities.

Europol pursues the strategy of “it takes a network to defeat a network”, and is therefore working together with law enforcement and private partners worldwide.

Crime-as-a-Service

Crime-as-a-Service is very relevant in regards to e-commerce fraud. It enables people that are not tech-savvy and actually don't have the technical knowledge to commit cybercrimes that require a certain level of technical understanding. Therefore it lowers the technical entry-barrier, as it supports and facilitates the creation of value chains.

The phenomenon is based on division of labour, different roles and specializations of individual members and groups, and the partnerships among them. It is very difficult to capture the underlying structures, as they often tend to be unstructured, and connections between actors or groups are often project- or only transaction-based. Therefore, due to the unstructured, often altering nature of the connections, they are difficult to investigate.

Some groups have a company-like structure, with executives and people specialized in technical tasks. There are marketplaces, similar to Amazon, where one can buy credit card data, even with a rating system, where the quality of the data and the seller can be rated.

It is not necessarily expedient to focus on taking out certain elements, such as botnets, as backup structures, and contingency and recovery plans are usually in place to ensure the service.

Therefore, it is important to see and understand Crime-as-a-Service as its own economy with specialized roles and dependencies. Based on their strategies, counter-strategies against Crime-as-a-Service are developed. By identifying choking-points, police work can be focused on certain services or actors, causing an impact on the economy when removing these services or actors.

One strategy is to act upon the reputation of certain actors. Due to anonymity, the name of a certain actor (such as a seller of credit card data) and its reputation are essentially the only things the business is based on. By damaging the reputation, the economic viability is likely to be negatively influenced. Another strategy is to interfere with the underlying price model to change the price structure.

It is also important to be present in the Darknet and other underground networks, in order to be able to learn of new developments, as well as to create certain nervousness among the actors.

Another prevention strategy of Europol is to create programs, which aim to target young talents, often with a playful approach. Their purpose is to prevent them from drifting into cybercrime by sparking their enthusiasm for the positive aspects regarding their talent.

A.2.3 Investigator of Criminal Intelligence Service Austria

Agency	Criminal Intelligence Service Austria
Department	Economic Crime
Date & Time	11.07.2017, 10:00-11:00

General

The Criminal Intelligence Service Austria is the central department of the criminal investigation police. Their main area of responsibility is the coordination of criminal investigations in Austria. Due to their central position in investigations, they keep an overview and are able to identify connections between cases. Usually, they are not involved in operational investigations, with the exception of special commissions. Another area of responsibility is the international co-operation and the correspondence with other countries (such as gathering information regarding an investigation from another country), which is solely handled by them. One of their departments is solely concerned with credit card fraud and similar types of fraud.

A further increase of e-commerce fraud is to be expected. This is due to the general increasing volume of e-commerce, but also due to new technologies and services that are continuously developed and invented, which provide new ways to commit fraud.

Five classes of fraudsters can be distinguished: (1) People who are not solvent, but order products online for their own personal use. They almost entirely use payment after delivery, and are not very sophisticated. It can be compared to a modern, online version of shoplifting. (2) Organized groups residing in Austria, which typically use payment after delivery; also acting with a low level of sophistication. They sell the fraudulently acquired products amongst their circles of friends and acquaintances, or via online platforms. (3) Criminal groups, also located in Austria, which use payment after delivery and stolen credit card information to commit fraud. (4) Criminal groups from abroad, where members move to and respectively register their residence in Austria. These fraudsters order numerous products within a short time, mainly using stolen credit card information, and leave the country afterwards. (5) Criminal groups from abroad which are highly sophisticated and involved with Crime-as-a-Service, which make use of provided criminal services: purchasing credit card data, Reshipping-as-a-Service, and services to disguise their tracks and real identities. They target high-quality products using stolen credit card information.

Popular products for e-commerce fraud are clothing (mainly branded clothes), shoes, smartphones and other electronic devices (such as notebooks or navigation systems). Their focus is on products that can be sold easily. Typically, the value of a fraudulent e-commerce order is on average between 100 and 200 Euros, expensive goods are the exception. The majority of fraudulently acquired products remains in and is sold in

Austria. High-quality goods are mostly transferred to another country, usually by making use of so-called packet mules.

Facilitating factors of e-commerce fraud are the generally high volume of transactions, the majority being legal transactions, as well as the ease in which fraud can be committed. For example, payment after delivery is very susceptible to fraud. It can be committed by using fantasy names or someone else's identity, for example by simply using the information that can be found in a phone book. Another facilitating factor is the disguise of tracks, such as the use of e-mail addresses of free e-mail providers or measures to hide the real IP address.

In Austria, most cases of e-commerce fraud are committed by using payment after delivery, followed by fraud committed by using stolen credit card information. Cases of e-commerce fraud with other means of payment are rare. Criminal groups from abroad are usually located in Russian-speaking regions.

Countermeasures

Prevention measures and the monitoring of transactions by merchants are very important in order to counter fraud attempts, i.e., to prevent e-commerce fraud before it occurs.

There are various challenges regarding countermeasures: For merchants, customer satisfaction is imperative. Customers want fast and simple processes and services, therefore merchants strive to satisfy their requirements. One example is 3D Secure, which would increase the security of credit cards, but many customers refuse to use it. Another example are reception boxes, where packages can be picked up anonymously and around the clock. This is convenient for customers, but considered another weak point for preventing fraud. Additionally, not only is the number of merchants increasing, new services are continuously being introduced, allowing for new ways to attempt fraud. Moreover, it is easy for fraudsters to use stolen or forged information, but it is difficult or unfeasible for merchants to check the legitimacy of the entered data.

As long as merchants' losses due to e-commerce fraud are manageable, and merchants are still able to generate profit, they will continue to offer their services and focus on customer satisfaction, thus neglecting further security measures. Besides this, the invention of additional security measures by individual merchants poses the risk of customers migrating to other merchants.

In theory, it could be possible to eliminate e-commerce fraud completely, but this would require payment mean adjustments in order to make them more secure, as they are the weak link. However, in practice it is not possible to eliminate it completely; therefore, the objective must be to make it more difficult for fraudsters. This can be achieved with additional security measures for payment means.

It is quite common that vulnerabilities are exploited until a certain point is reached, which consequently triggers countermeasures. For example, the skimming of credit cards, where cases increased to an amount that required measures to be taken to prevent it.

As a result, Geoblocking was introduced, which had a huge impact on skimming, and reduced the number of cases significantly. It is conceivable that this could be the case with payment after delivery as well. If fraudulent cases reach a certain point, effective countermeasures may be made necessary.

Investigations

Many cases of e-commerce fraud are not reported. On the one hand, this is due to the monitoring of merchants, where a part of the fraud attempts is already detected. On the other hand, it is quite common for merchants to only report cases exceeding a certain limit. Cases with a lower loss are often not reported, as it would require additional resources (file a report, provide data, etc.), therefore merchants tend to accept these losses. The victims themselves report cases of identity theft, which is of relevance regarding payment after delivery.

All cases that are reported are followed by investigations, independent of the amount of loss or if an attempt was successful or not. In Austria, the police is obligated to investigate a report, whereas some other countries handle it differently (for example, in the UK cases of fraud are only investigated if exceeding a certain amount of loss).

If the fraudsters are from abroad, which is usually the case with fraudsters of class four and five (cf. above), investigations are much more difficult. Investigations in other countries require correspondence with the respective local authorities. Therefore, it is an additional hurdle for investigations: The correspondence must be initiated at the particular channels at Europol or Interpol to receive support or responses to inquiries from local authorities of the respective country. The correspondence must often be translated to the official language of the respective country, which further adds to the effort and delay.

The complexity of investigations also depends on the type of co-operation. In the case of inquiries (for example, to get the information if a certain person is already known to the local authorities) the co-operation works unproblematically, as the communication channels and contact points within the networks of Europol and Interpol are already specified. Cases with ongoing investigations in co-operation with other countries over a longer period are more complex, such as investigations against offenders which are located abroad but committed cases of e-commerce fraud in Austria, where the investigations are undertaken jointly with the local authorities (identify offenders, search for and seize evidence, arrest offenders, etc.).

Evidence in cases of e-commerce fraud is commonly the delivery addresses. Additionally, they request all related data of an order from the respective merchant. However, the data is often not useful, due to the use of e-mail addresses of free e-mail providers or the usage of means to disguise the IP address. Moreover, IP addresses usually don't lead directly to a person, but to a provider, making it necessary to make an inquiry for further information. In cases of drop-off locations, camera surveillance (if existent) can be helpful as well.

The higher the sophistication of a criminal group, the fewer usable tracks are left behind. Usually, useful tracks only lead to low ranking members of these groups, not to their leaders. In contrast, ordinary fraudsters often don't even have the know-how to disguise their tracks, making investigations easier.

A problem regarding investigations is that there is often a delay between the time when the fraud happens and the time of the report. Due to the delay, it can happen that certain tracks are no longer available. Therefore, co-operation with the private industry is important for investigations, for example with merchants and logistics providers, to be able to respond to e-commerce fraud in a timely manner.

In every district throughout Austria there are 2-3 investigators with specialized IT training, who are responsible for recording traces in crime cases where computers are involved.

In a large number of cases of e-commerce fraud, the investigations are successful.

Currently, a system has been developed to collect and analyse all cases of fraud in Austria to help recognize trends and connections between cases, that will allow officials to track down criminal groups.

Crime-as-a-Service

Crime-as-a-Service has a big impact on e-commerce fraud, especially criminal groups from Russian-speaking regions who are involved with and making use of it. As it is in the real economic world, company-like structures offer their illicit services to others, such as providing credit card data, phishing, or access to a network of packet mules. There are even translation services used, for example, to adapt phishing mails to the target region (as linguistic errors would raise suspicion among potential victims). Other services are concerned with disguising the tracks of a crime. Highly sophisticated criminal groups make use of these services to commit e-commerce fraud.

It is difficult to take actions against it, as the investigations are inherently cross-border. The Criminal Intelligence Service Austria is part of a large network with both Europol and other countries, where their co-operation works excellently. Due to these connections, it is often possible to achieve results and receive support within a short time. Outside the network, a close co-operation is more difficult.

These criminals and criminal groups are also keen on covering their tracks, which aggravates investigations even more. Additionally, the criminals often don't know each other personally and instead communicate with online nicknames, which complicates the discovery of their real identities.

Prevention measures, especially information campaigns are important and can have a huge impact. It is necessary to inform the general public about certain criminal schemes, such as the packet mule scheme. If citizens know about it and don't fall for it, it can also have an impact on e-commerce fraud on a large scale. If operators of this scheme realize

that it is becoming increasingly difficult to recruit packet mules in Austria, it might make it necessary for them to give up targeting Austria, and target other countries instead.

A.3 Interview with expert from payment provider

A.3.1 Focus areas of the interview

- **General**
 - Development of e-commerce fraud
 - Facilitating factors
 - Affected products
- **Payment service**
 - Fraud characteristics
 - Vulnerability of payment method
- **Countermeasures**
 - Measures
 - Challenges
- **Investigations**
 - Reported cases
 - Experience

A.3.2 Payment provider for payment after delivery

Position	Head of Risk
Payment method	Payment after delivery
Date & Time	02.11.2017, 9:00-10:00

General

It can be expected that e-commerce fraud will continue to increase in the future; the numbers are rising since the emergence of e-commerce, and this development will continue.

Reasons for this expectation are, among others, that each new system that comes into play provides new ways to exploit them and enables fraudsters to discover new fraud strategies. It is a game of cat-and-mouse, as it seems that fraudsters are always not only one but two steps ahead. They form groups and networks, exchange information, and always find ways to commit fraud.

What adds to the challenge is the need for finding a balance between making a system safe while still providing a system for customers that is easy to use, fast, and customer-friendly. Accordingly, the faster the processes and the more volume of transactions, the higher the risk of fraudulent transactions.

Another facilitating factor for e-commerce fraud is that people are often not careful enough with their sensitive data due to a lack of basic knowledge about data protection.

Another big issue regarding e-commerce fraud is the delivery risk, which comes in handy for fraudsters. Parcels are often left at the doorstep or retrieved without the necessity of showing a personal ID. In general, the “triangle” payment provider, merchant, and delivery service and their different interests (for example, the merchant wants a shipment to be as cheap as possible, therefore often waiving shipping insurance, while the delivery service is concerned with delivering a parcel preferably in the first delivery attempt, while the payment provider prefers insured shipment and delivery to the intended buyer) cause additional issues.

Products most affected by e-commerce fraud are those with a high value that are easily resellable on black markets or online market places.

The majority of fraudulent transactions processed by the them are based on identity theft; cases of friendly fraud are generally low (and usually with low-level amounts).

Payment service

The information needed from a customer for payment after delivery is very basic: name, surname, date of birth, e-mail address, and address. Therefore, it is the easiest way to commit e-commerce fraud. Payment after delivery usually requires much less information than, for example, payment with a credit card.

It is necessary for them to check two types of risk: the credit risk, which requires an estimate of the liquidity of a customer, and the fraud risk, which is necessary to determine if a transaction is legit or fraudulent. They guarantee the payment for merchants regarding the credit risk (i.e. if the check shows that a customer is creditworthy, the merchant receives the payment even if the customer is not able or willing to pay), but this guarantee does not cover cases of fraud. However, as it is not always clearly distinguishable, it is often required to find an agreement with a merchant in cases of fraud. In cases of suspected fraud, merchants always have to provide the invoice that was sent to the customer as well as the proof of delivery of the shipment.

The more data they have, the better they can estimate the fraud risk. Therefore, they try to get as much information as possible, such as the IP address, or a device ID, from internal and external systems. Thus, depending on a merchant and how their system is integrated into the system of the merchant, they receive additional information that can be used for fraud examination purposes.

Their payment service is only provided to end customers resident in the DACH region (otherwise there would be no way to control the risk, as credit checks would not be feasible). According to past experience, there were not many cases where packet mules were involved.

Countermeasures

The most important factor in their efforts against e-commerce fraud is analysing what is going on via real-time monitoring and what has already occurred, thus learning from mistakes in the past and deriving patterns that can be used to detect e-commerce fraud in the future. A multitude of patterns have already been revealed and used to determine rules for their rule-based fraud detection systems.

The revealed patterns are often very specific, and depend on factors such as merchant or country. For example, one of the revealed patterns showed the usage of deceased identities at a specific merchant (which worked well until uncovering the scheme: credit check companies need some time to update their data, which was exploited by a fraudster; additionally, the identities of elderly people were used because they usually possess a good credit score).

The issue with countermeasures is that one can only be really sure if it is a case of fraud once it has already happened. Therefore, it is important to catch fraudulent transactions before the goods are shipped. Once the goods are shipped, the percentage of cases where goods are returned is very low.

They use information from various external sources, such as device fingerprinting and e-mail verification services, to get a comprehensive picture about a customer and the underlying transaction.

They use an internal and an external rule-based system; both are used to determine a risk score per transaction. The rules cover comprehensive factors of a transaction, such

as the value of the shopping basket, geographical information, or its velocity.

To be able to handle the increasing volume of transactions in the future, the use of systems based on machine learning is also considered.

It is important to find the right amount of countermeasures, as it is required to have a payment system that is not too complicated and still customer-friendly. Additionally, it is also a matter of costs, as each system used to prevent or detect fraud adds to the costs per transaction as well as total costs. Thus, it is not worthwhile to eliminate e-commerce fraud entirely, as it would be at the expense of customer satisfaction and would create costs that far exceed the profit per transaction.

They offer the option that allows end customers to verify their identity via an online video ID check or by sending scans of identity documents. This proceeding is required in the case of a declined transaction (for example, in the case of a bad credit score), or, depending on the merchant, for high-value orders. This strategy is largely accepted by customers, as those who want to use their payment method are willing to undertake the identity verification. While it allows them to revert transactions that otherwise would have been declined, this strategy also proves to be effective against fraudsters, as they are commonly deterred by identity verification measures.

The biggest challenge regarding countermeasures is that although it is easy to commit identity theft and identity fraud, it is difficult to verify the identity of a customer. Additionally, there will always be loopholes that can be exploited by fraudsters to commit e-commerce fraud.

Investigations

E-commerce fraud that makes use of payment after delivery is usually based on identity theft and identity fraud, meaning the victims are those whose identity is fraudulently used. Thus, victims have to report cases of fraud themselves, as it is not the obligation of the payment provider.

They support investigations by providing the related information: for example, purchase details (such as details about the purchaser and product information), the IP address, and other relevant data. In some cases of e-commerce fraud where fraudsters used their payment system, they were also invited as witnesses to court to give a testimony.

However, the impression is that reported cases are often not thoroughly investigated and eventually vanish in a drawer; thus it seems that investigations are hardly successful.

To not only improve investigations but also the combat against e-commerce fraud in general, they'd suggest to establish a network with law enforcement and other payment providers to be able to exchange information and stay up to date regarding upcoming fraud strategies.

A.4 Interviews with merchants

A.4.1 Focus areas of the interviews

- **General**
 - Extent of e-commerce fraud
 - Affected products
 - Facilitating factors
 - Cases of loss
- **Characteristics**
 - Agreement
 - Payment
 - Delivery
- **Countermeasures**
 - Prevention measures
 - Detection measures
 - Effectiveness of current measures
 - Enhancement of countermeasures
 - Challenges and problems
- **Investigations**
 - Reported cases
 - Experience

A.4.2 Merchant #1

Position	Sales and fraud manager
Company size	Small (<20 employees)
Sector	Electronic goods
Date & Time	13.06.2017, 10:00-11:00

General

Cases of fraud attempts are generally low (about less than 1%), and completed cases of fraud are very rare.

Products that are most affected by fraud attempts are high-end products, especially iPhones and Macbooks.

The main facilitating factor for e-commerce fraud is the naivety of people: On the one hand, many people are not taking enough care of their payment details. In many cases, victims expressed that they were called and asked to participate in a survey, during which they were asked to provide their credit card details and the secure code, which they willingly did. On the other hand, in most cases of fraud, so-called reshipping mules were used, i.e. people who are naive enough to reship fraudulently ordered goods while thinking to pursue a decent job.

They make sure to fulfil the compliance rules of the respective payment means so that potential losses are covered by the payment facilities due to seller protection programs. In four years, there were only two cases of fraud where they had to bear the losses.

Characteristics

Most fraud attempts show a certain indicator: Although the fraudsters appear as Austrians, and use shipping and billing addresses located in Austria, they use e-mail addresses that suggest that they are from another country, in most cases from Germany. This is due to two factors: Firstly, fraudulently used means of payment are in most cases from German people. Secondly, in most cases fraudsters use reshipping mules from Austria to receive and reship the goods.

The majority of fraud attempts are committed with credit cards (about 9 of 10 fraud attempts). After the integration of PayPal there was a peak in fraud attempts with this payment method, but it declined after some time. All fraud attempts target products that are in stock.

Moreover, fraudulent orders are never directly delivered to a recipient, but rather dropped off at reception boxes. This is due to redirection of the delivery or by making sure to use addresses where no one would accept the delivery, such as empty flats, where they are then picked up by a fraudster or a mule.

Counter-measures

Customers who pay with debit or credit cards have to enter their 3D Secure code. In the case of cards that don't have a 3D Secure code, a manual request is sent to the issuer of the card to verify the data entered by the customer. This ensures that customers fulfil the guidelines of the credit card issuers, and are protected if a transaction turns out to be fraudulent. As the verification request can take up to 1-2 days, they only make exceptions for regular, reliable business customers and refrain from verifying the payment.

In cases of payments via PayPal, it is important to make sure that the delivery is only sent to addresses that are saved in the PayPal account. This is done manually by comparing the entered shipping addresses with the PayPal addresses. The address check, as well as other measures, makes sure that they are protected by the seller protection program of PayPal and losses are covered in cases of fraud. This check can be done immediately and does not (or only minimally) delay the processing of the transaction.

Payment after delivery is not offered, as it seems like an open door for fraud attempts, although customers frequently request it. Exceptions are only made for regular business customers with a reliable customer history.

They rely solely on the manual review of orders (check of e-mail address, check if shipping address and PayPal address match, manual request for verification in cases of credit card payments without 3D Secure code). Even if the volume of transactions were to increase, the fraud detection could still be handled manually. In the case of a dramatic increase, it would require additional human resources.

The merchant has developed a tool to save information about each customer and their transaction history, which allows them to take steps accordingly if a customer shows suspicious behaviour.

Deliveries are almost entirely shipped with a tracking code and insurance up to a certain value. Only in rare cases are goods sent via letter (no tracking or insurance), and about every fifth case claims to not have received the delivery. These cases are tracked in their self-developed tool and used to take measures if a customer repeatedly claims to not have received deliveries.

Overall, they estimate that the effectiveness of their prevention and detection measures is about 99%.

One of the challenges is customer convenience and customer satisfaction: For example, even though 3D Secure strengthens the security of a payment, most customers dislike the additional effort. This demonstrates the risk of deterring customers due to additional effort, while at the same time measures against fraud have to be taken. In general, it would be necessary to induce a raised awareness in people to keep their payment details safe and to not fall for schemes that sound too good to be true. One problem in this regard could be that account holders and card holders are to the greatest extent protected by insurances and protection programs of the payment facilities, therefore the motivation to take more care regarding the security of payment means is negligible.

Another problem is the usage of reception boxes. It would generate additional costs to prohibit that a delivery be dropped off at a reception box, which is uneconomically due to the generally low margins in e-commerce.

A general problem with fraud is that it generates effort, thus it causes costs and is time-consuming. However, most transactions are legitimate and only rare cases are indeed fraudulently.

Investigations

In the last four years, they reported about 40 cases to the authorities. In some cases, they were asked to provide data about the fraud case.

Generally, they have the feeling that these cases peter out. So far, they only received letters with the information that the investigations were discontinued in about 10 cases.

A.4.3 Merchant #2

Position	E-commerce manager
Company size	Medium (<50 employees)
Sector	Multimedia and electronic goods
Date & Time	29.06.2017, 10:30-11:30

General

The cases of fraud are less than 0.5%. Due to the generally increasing e-commerce volume, they also expect an increase of the number of fraudulent e-commerce transactions in the future, but with a stable ratio.

Most affected by e-commerce fraud are typically multimedia products and electronic goods. Smartphones (mainly high-end smartphones such as iPhones) and games consoles are especially affected.

They offer payment after delivery, and payments with credit cards and via bank transfer. In about 60% of orders, payment after delivery is used. The usage of credit cards sums up to approximately 10-15%, while bank transfers make up the rest. E-wallets are not supported, as they are not in demand by their customers.

A major facilitating factor of e-commerce fraud is the balance between customer satisfaction and measures against fraud. Although payment after delivery poses a high vulnerability to fraud, it is heavily demanded by their customers. By not offering this mean of payment they would certainly risk the loss of customers. Moreover, they allow customers to order products as a “guest”, i.e. without registering an account. This is also requested by some customers, probably due to data privacy concerns, but it simultaneously provides more anonymity for fraudsters.

For payment after delivery, they use the service of a payment provider, who does not only undertake the handling of invoices and payments, but also reviews orders and conducts risk assessments. They have an agreement with the payment provider, which clearly states the guidelines regarding the duties of the payment provider (how the review and risk assessment has to be done) and the duties of the merchant. In cases of fraud, based on the agreement, it is decided who has to bear the losses.

Characteristics

Shopping cards with anomalies are good indicators for fraudulent transactions. It includes orders with values exceeding a certain limit, specific products, or the order of several items of the same product (such as several items of the same smartphone model) or same product type (like several smartphones). It also raises suspicion if the entered data does

not seem to match the ordered products (for example, an elderly person ordering a games console).

Additionally, the data entered by fraudsters, such as names or e-mail addresses, often indicate a fraud attempt as well.

Most of their fraud cases are in conjunction with payment after delivery. They have hardly experienced any fraudulent transactions with credit cards and no cases with bank transfers.

Recently, they noticed an increase of fraud cases where the orders are dropped off at reception boxes.

Counter-measures

The review of an order and the risk assessment of the payment provider for payment after delivery comprises a credit assessment and checks regarding the integrity of the entered data with data from various sources (such as validation of the address and age of the e-mail address). Based on this information, the payment provider determines whether an order should be rejected or accepted.

Additionally, and even in the case of the approval of the payment provider, they carry out manual checks for orders fulfilling specified criteria, such as the value of an order exceeding a certain threshold.

Currently, the measures against fraud are sufficient. It would be desirable to decrease the cases of fraud even more, but the cost-benefit ratio is also of importance. Moreover, the introduction of additional measures could negatively impact the customer satisfaction, and result in a loss of customers.

Due to the low quantity of fraud cases with credit cards, they have not yet considered introducing 3D Secure.

Orders are solely shipped with a tracking code and insurance up to a certain value. Shipping is restricted to Austria. As an additional service, they offer the option for customers to pick up orders at their stores. In this case, the order is handed over to the buyer only, and the identity is verified by checking an ID.

Investigations

Most of their orders are paid by payment after delivery, and the majority of fraudulent cases is caused by this payment method. Due to the nature of payment after delivery, it is not their responsibility to report these cases, and they are, naturally, not even aware of them (otherwise these orders would be rejected). The victim is the person whose identity is stolen and fraudulently used, therefore the victim has to report it to the authorities.

In cases of reports, they were asked by the authorities to provide the data related to these offences. In some cases, they were witness in a trial against a fraudster.

Investigation in the Darknet

B.1 Addresses of hidden service

B.1.1 Search engines

- **Candle**
gjobqjj7wyczbqie.onion
- **not Evil**
hss3uro2hsxfogfq.onion
- **Torch**
xmh57jrznw6insl.onion

B.1.2 Directories

- **Fresh Onions**
zla132teyptf4tvi.onion
- **Hidden Wiki**
hwikis25cffertqe.onion
- **The 2017 Verified Hidden Wiki**
wikiti3e4q2ca2e7.onion
- **The Hidden Wiki**
zqktlwi4fecvo6ri.onion
- **The Uncensored Hidden Wiki**
gxamjbnu7uknahng.onion

- **UnderDir**
underdj5zi0v3ic7.onion

B.1.3 Forums

- **CLUB2CRD**
Forum mainly used for offering illicit services. Bi-lingual community (Russian and English, posts in English prevail). Also available on the Surface Web (sky-fraud.ru).
crdclub4wraumez4.onion
- **ShadowCrew**
Community mainly concerned with carding and fraud topics. Focused on exchanging information; many tutorials are provided.
shadowjxlhyj4gf.onion
- **SKY-FRAUD.RU**
Forum for cybercrime in general, including carding. Bi-lingual community (Russian and English, the majority of posts is in Russian). Also accessible on the Surface Web.
bcbm4y7yusdxthg3.onion
- **The Onion Forum**
General forum for cybercrime topics, mainly concerned with carding. Also used for trading.
onion4dtkkeyk7f2.onion
- **GGMCCLOUD1**
Carding forum with monthly membership fee.
5jlofek2ajaywwk3.onion
- **Kickass**
Carding forum with one-time membership fee.
kickassugvgoftuk.onion
- **Omerta**
Carding forum with one-time membership fee.
omertavzkmsn6tp6.onion
- **Tor Carding Forum v3**
The Darknet site is only used for referencing to the domain on the Surface Web (<http://carderforum.su>).
torcrdttg6e4opr.onion

B.1.4 Marketplaces

- **Dream Market**
lchudifyeqm4ldjj.onion
- **Silk Road**
silkroad7rn2puhj.onion
- **Tochka**
tochka3evlj3sxdv.onion
- **Trade Route**
vca2j25eszpdzurk.onion
- **Valhalla**
valhallaxmn3fydu.onion

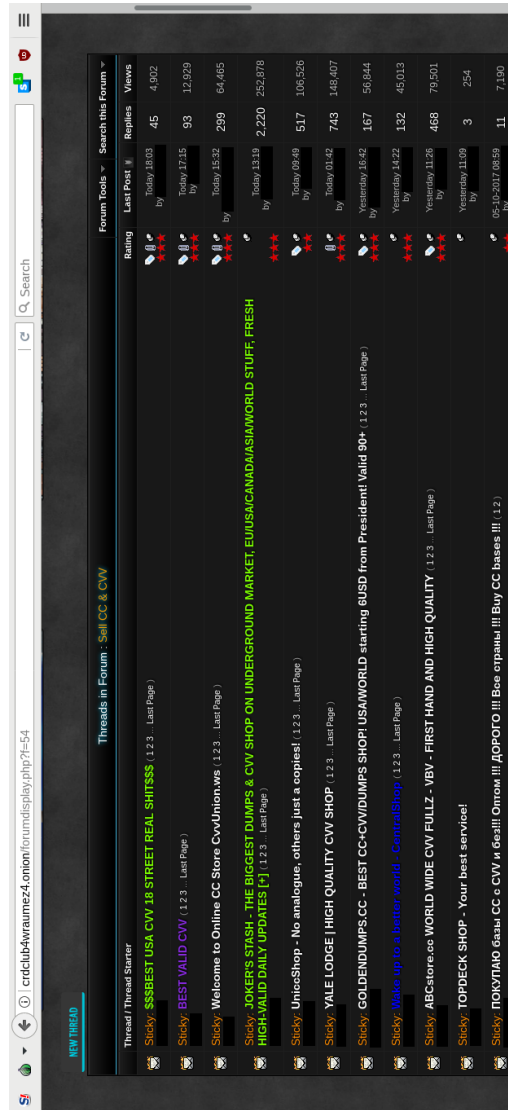
B.1.5 Shops

- **7YearsinTibet**
Credit cards, PayPal accounts
7yearjhcbetzyo6t.onion
- **Cash Machine**
Credit cards, PayPal accounts, bank accounts
hcutf6eapjll2gqk.onion
- **MrRobotShop**
Credit cards, PayPal accounts, bank accounts
hhuwppvm3fbuipb.onion
- **netAuth**
Credit ards, PayPal accounts
netauth3qialu2ha.onion
- **Reborn Market**
Credit cards, PayPal accounts, verified accounts for Amazon and ebay, bank
accounts
yh3yhsamn65x3xe2.onion
- **TGSS Carding**
Credit cards, PayPal accounts, gift cards (e.g. Amazon, iTunes, Google play)
giftcardmzsfdsxq.onion
- **VendorPro**
PayPal accounts, bank accounts
vendpmmhx5ylctjf.onion

B.1.6 Other hidden services

- **Hidden Answers**
Q&A community
answerstedhctbek.onion
- **KINDLES - Carding lessons**
Courses to learn carding (“Jump from noob to the next level in no time”); three courses are offered: carding lessons, Paypal lessons, full carding lessons (i.e. extensive carding and PayPal skills).
purpleum5m4w5jf5.onion
- **Carders University**
Various courses are offered, including courses to learn carding and cashing out PayPal accounts.
c7pt6x3bpvyq4ahk.onion
- **Hansa Market (seized)**
Hidden service of the Hansa Market which was seized as part of Operation Bayonet and taken over by the Darkweb unit and National High Tech Crime Unit of the Dutch National Police.
hansamkt2rr6nfg3.onion
- **Hidden service of the Police and the Judicial Authorities of the Netherlands**
Publication of usernames of Dutch vendors and buyers from the Hansa Market identified by the Darkweb unit of the Dutch National Police.
politiepcvh42eav.onion

B.2 Screenshots

Figure B.1: Adverts for credit cards at the *Club2CRD* forum

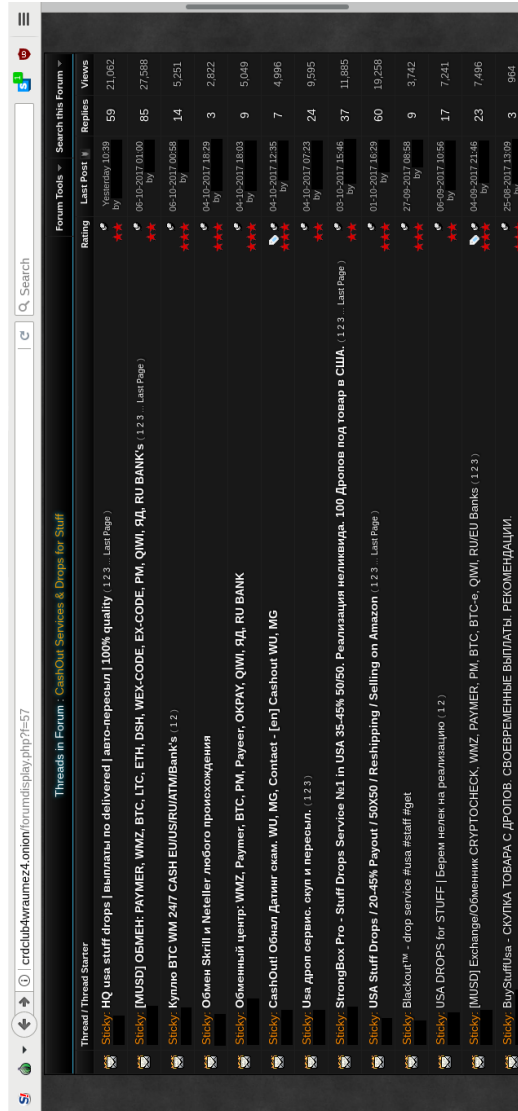


Figure B.2: Section about cash-out services and drops for stuff at the Club2CRD forum

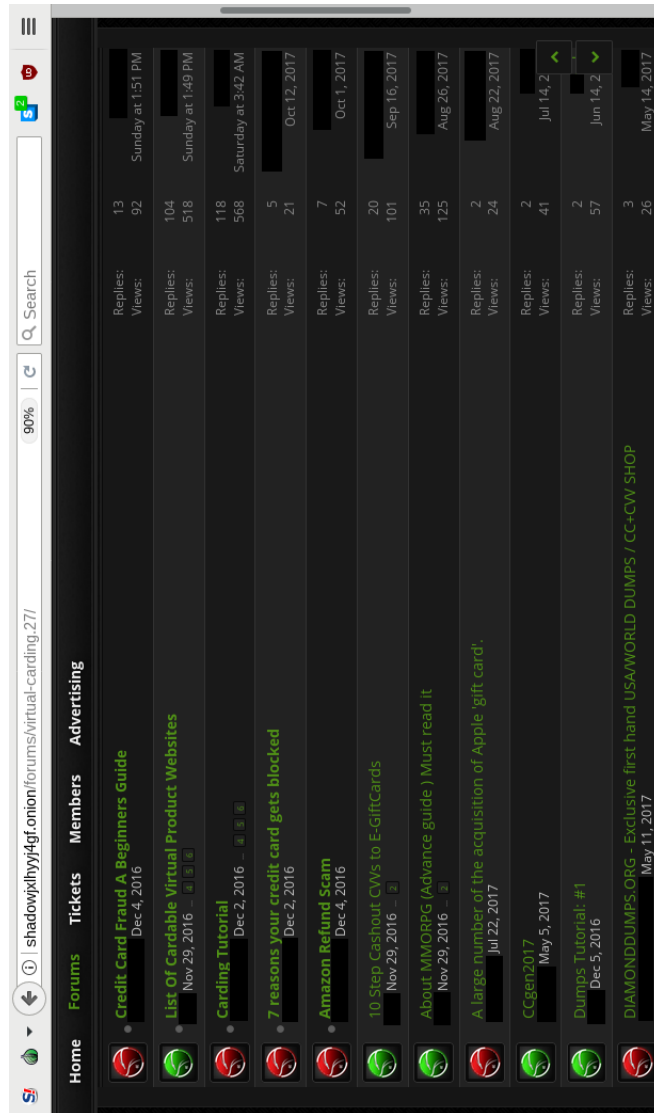


Figure B.3: List of some of the available tutorials in the virtual carding section at the ShadowCrew forum

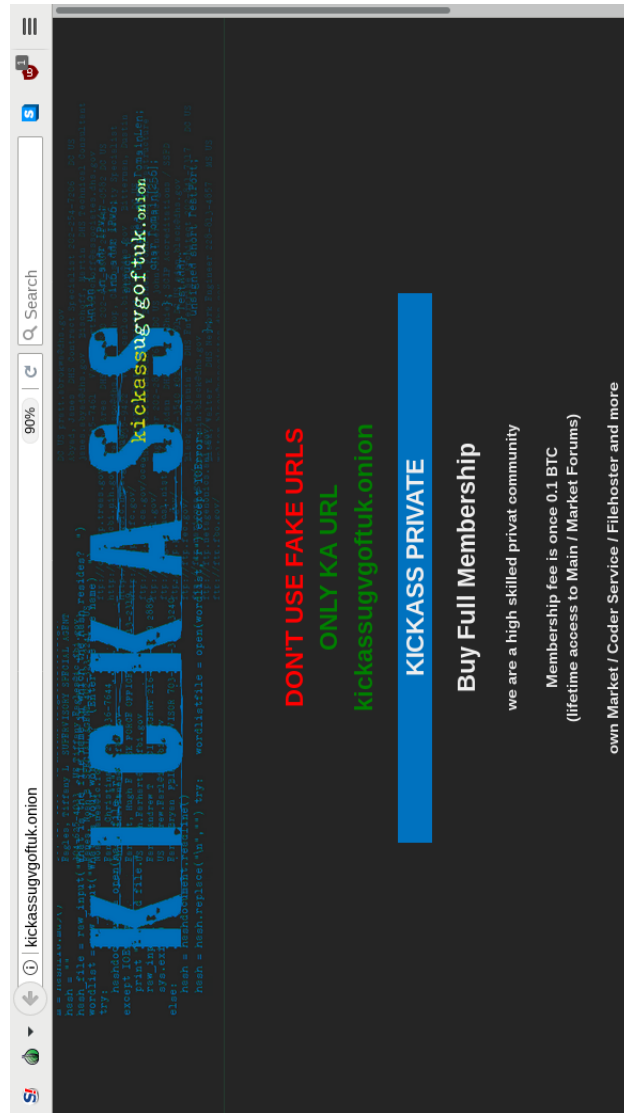




Figure B.4: Information about the membership fee for the *Kick Ass* forum



Cash Machine™ For Everybody!
 Best Solution to get Money Quickly

- ✓ **Fresh and New Accounts** Every Day !
- ✓ Different Balances and Prices **Available**
- ✓ All our Goods are **100% Verified**
- ✓ **Free & Clean** socks5 for each account (in the same Town as the Holder)
- ✓ All Accounts have the **Balance Mentioned** and are Linked to **Bank Account** and **Credit Card** of the owner
- ✓ **Account Replacing** if Amount is Different than what We ve Agreed
- ✓ **Complete Step by Step** Walkthrough Guide (Very Easy Cash Out!)
- ✓ Cashing Out **WORLDWIDE** in **Less Than 4 Hours**

1st
Deep Web

What do you need ?

EU Credit Card x 20 full info 1500€

Email (You will receive every order by email)

Buy now !

Figure B.5: *Cash Machine* - shop for purchasing credit cards, PayPal accounts and pre-paid cards



CC's are delivered like this:
IBAN | CW/CW2 | EXP DATE | NAME | ADDRESS | CITY | STATE (USA) | ZIP | COUNTRY | MMN | DOB | SSN (USA) | PHONE | EMAIL |

USA CC Fullz + tutorial

EU CC Fullz + tutorial

Your email (You will recieve CC by email)

[BUY](#) (no javascript)

PAYMENT METHOD: Bitcoin - After sending funds you will have to wait for 4 network confirmations and than check Your email.

Figure B.6: Order process at the *7YearsinTibet* shop

AUTOMATED PAYPAL AND CREDIT CARD MARKET.

YOUR ORDER IS - IN PROGRESS

- (1) SEND EXACT BTC AMOUNT TO [REDACTED]
- (2) WAIT FOR 4 BITCOIN NETWORK CONFIRMATIONS & CHECK YOUR EMAIL
- (3) Recieve Credit Card details



[back to main page](#)

Figure B.7: Payment process at the *7YearsinTibet* shop

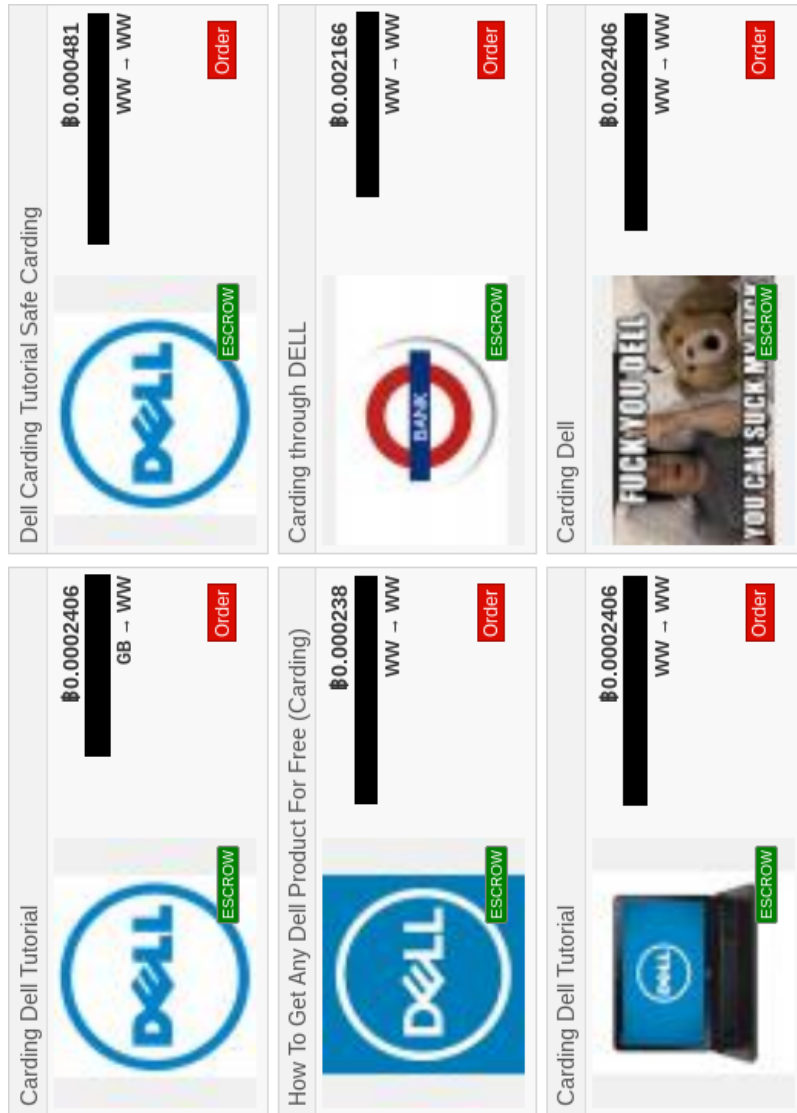


Figure B.9: Tutorials for carding Dell (offered at the *Dream Market* marketplace)

amazon carding 2k17 (Updated method)

Price: \$ 5

Vendor: [View Listings] [REDACTED]

Payment method: **Escrow**

Ships From: Not Specified

Category: Drops

Stock Remaining: 9999

+1448, 35, 98% Level 2 ★★ PGP Verified


amazon carding 2k17 (Updated method)

If your old method of carding Amazon has been shielded or doesn't work then this is the license for you.

HOW TO MAKE some extra \$\$\$\$\$\$\$\$ Give away prices for 2017 tutorials. These tutorials are upto date and have been tried and tested. We try as much as possible to make them n00b (newbee) friendly. If you do not understand something in them then do some research (google is always there to help you). Understanding the procedures in the tutorials and following them to the letter is the key to making \$\$\$\$\$\$\$ Carding and It is very popular these days. Today everyone wants to be a successful Carder and there are million of different carding methods. Knowledge is power so we don't only provide you with carding and paypal methods we also provide you with useful tips on how to go about this successfully. NO REFUNDS WE AREN'T HERE TO TEACH YOU IF YOU HAVE DIFFICULTIES THEN GOOGLE IS YOUR FRIEND. NO STUPID MESSAGES IF RECEIVED USER WILL BE BANNED FROM PURCHASING FROM US.

Figure B.10: Tutorial for carding Amazon (offered at the *Silkroad* marketplace)

Listing
Feedback (131)
Discussion (8)



Paypal Account.
Accounts&Drops

★★★★★

Multilisting

Excellent stock

Shipping from: Undeclared
Shipping to: Undeclared

Secure payment option

Manual dispatch 8

Select the quantity

1

Select your shipment method

Do you have a discount coupon?

BUY

i have more than 10k of paypal account info. (Canada, UK, France, USA)
i'm selling the login and password+ victim ip + user agent.
available country (USA/CANADA/UK/FR/BE)

Figure B.11: Offer for PayPal accounts at the *Trade Route* marketplace







	1 x US GOLD CREDIT CARD ***** FRESH CARDS	13.59 EUR	██████████
	1 X EU CREDIT CARDS ***** FRESH CC	21.23 EUR	██████████
	♣ 1 X US CC ♣ 97% VALID RATE	13.59 EUR	██████████
	1 X US CC FULLZ - DOB + SSN	24.63 EUR	██████████
	1 x FR CC	25.48 EUR	██████████
	♣ 1 X NON AVS Credit card ♣	21.23 EUR	██████████

Figure B.12: List of credit card offers at the *Valhalla* marketplace

You don't have enough funds for this product. Start by loading balance to **your account**.

1 X UK CC FULLZ - DOB + SSN

29.72 EUR (0.008102 BTC)
more than 25 pcs in stock

Netherlands → Worldwide

PM (included)

1

Buy

1 fresh UK CC FULLZ - DOB + SSN.
HIGH QUALITY CCS.
PRECISE ME WHEN YOU ORDER IF YOU WANT VISA OR MASTERCARD OR AMEX
NOT CHEAP CC'S THAT BEEN SOLD HERE (SAME CC SOLD TWICE = BURNED)

Card infos :

- **** Card Numbers
- **** Expiration
- **** CVV/CVV2
- **** Date
- **** Name and Surname
- **** Complete Address
- **** Phone Number
- **** DOB
- **** SSN

Figure B.13: Offer for credit cards ("fullz") at the *Valhalla* marketplace

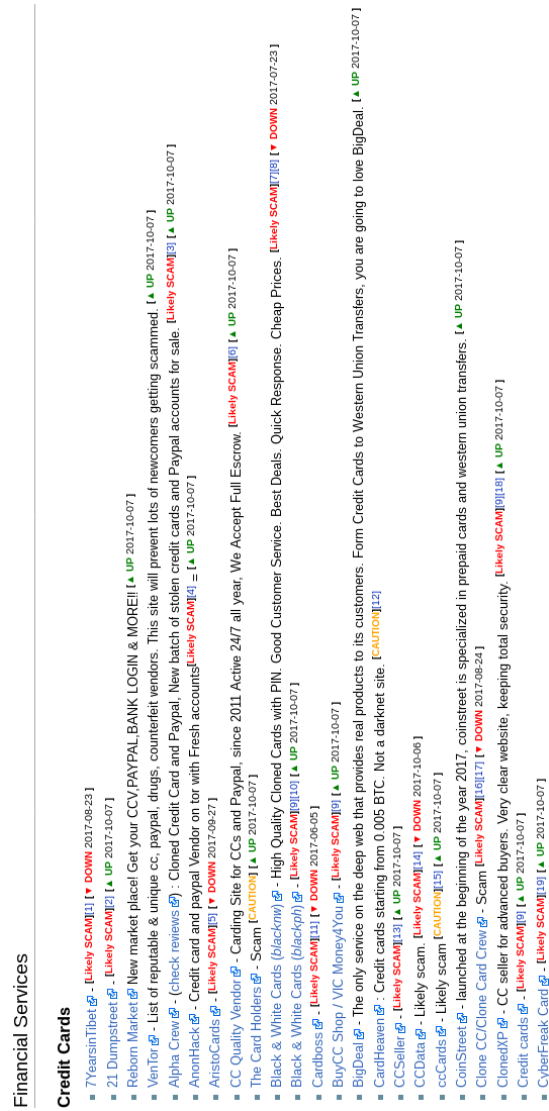


Figure B.14: Rating system in the *Uncensored Hidden Wiki* showing the high number of shop scams

0
1

The Hidden Wiki is probably a good place to start. There you can find some links to some stores (which are usually not scams) in category "Commercial Services".

answered 5 days ago by **N00b 101** (220 points)

[edit](#) [hide](#) [ask related question](#) [comment](#)

Wrong advise, they are usually ALL scams!!!

commented 5 days ago by **Experienced** [reply](#)

Figure B.15: Comment at *Hidden Answers* pointing out that links to shops in the *Hidden Wiki* are usually scams

CARDING LESSONS
Price: \$225
Basic OPSEC, Ip leak protection, how to use CCs to card items, types of CCs and checkers, and much more

PAYPAL LESSONS
Price: \$300
You take a fresh PayPal account and buy BTC without verifications from an exclusive shop. How to create stealth PayPal account. How to ATO a hacked account, and much more

FULL CARDING LESSONS
Price: \$800
become a master carder and learn everything about credit cards, paypal, creating drop bank accounts, making fake webstores, Stripe, Venmo, sources to buy dumps+pin, skimmers, emv/pos softwares and much more

Figure B.16: Description of carding and PayPal lessons offered by *KINDLES*

ALL COURSES

- » Security Mastery
- » Financial Institution Mastery
- » Money Trans Hack
- » Credit Carding
- » PayPal Domination
- » Onion Business
- » DeepWEB Investments
- » GiftCard Mastery


ABOUT CREDIT CARDING COURSE


This course is perfect for students that are ready to enter the world of Carding. Carders University provides students with access to 5,000+ CVV underground shops, and 700+ direct Dealers that are willing to sell for as low as \$3 per fullz & \$25 per dump.


We also provide students with all the tools needed to be a successful Carder. Hack, Scrape, and gather your own fullz/dumps and even become a dealer. This course gives students endless possibilities.

For training purposes we provide students with active Visa, Mastercard, Amex, & Discover credit cards free of charge. When students complete this course, they will be ahead of the game and making income very fast.

We will provide all students with softwares, proxies, and services at no additional costs.







📅 Course Schedule

👤 Available Seats: 2

📅 01/05/2017

🕒 3 Days

[Enroll Now!](#)

Figure B.17: Description of carding course offered by *Carders University*

<http://purpleum5m4w5jf5.onion/>



▲ 1
▼ 0

Any experiences or impressions?

scam or not



asked Apr 19, 2016 in [Scams and scammers](#) by Apprentice (2,125 points)

[Answer](#) [comment](#)

4 Answers

▲ 1
▼ 0

Kude is a pro in carding and you can trust him for giving you some valuable information and lessons about carding.



answered Apr 20, 2016 by Master First-Class (12,935 points)

[ask related question](#) [comment](#)

▲ 0
▼ 0

They are legit and you can see few post from them about carding here.



answered Apr 19, 2016 by Senior (7,840 points)

[ask related question](#) [comment](#)

Figure B.18: Comments about the legitimacy of *KINDLES* carding and PayPal lessons at *Hidden Answers*

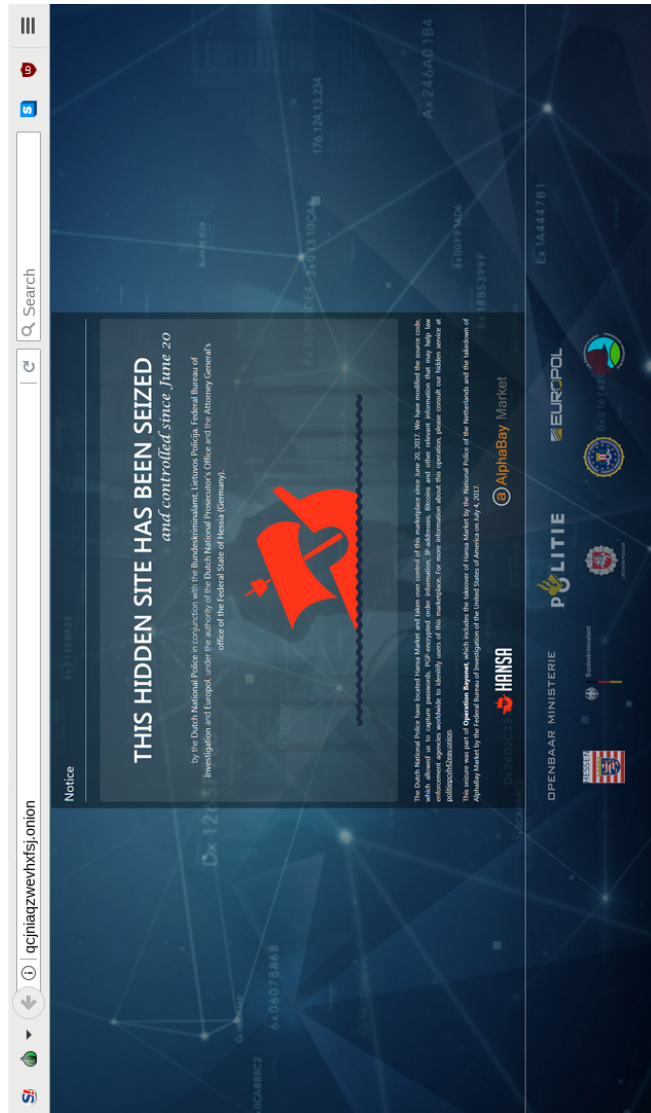


Figure B.19: Information that the hidden service of Hansa Market was seized by the Dutch National Police in conjunction with other law enforcement agencies

Active at Dark Markets? You have our attention.
 The Police and the Judicial Authorities of the Netherlands are active in the real world, but also in all corners of the Internet. We trace people who are active at Dark Markets and offer illicit goods or services. Are you one of them? Then you have our attention.

ACTIVE VENDORS

- rs6
- Dutchcandyshop
- DutchMagic
- DutchFarmerNL
- Klaasflakko
- WarnerBros
- FrankMatthews
- Hardquality
- HollandDutch
- AmsterdamConnection
- PartySquadNL
- QualityWhite
- DutchMasters

ARRESTED VENDORS

- QualityWeed
- HighQualityTrips
- RuudNL
- XTCEexpress
- TheHeineken
- AmsterdamUnited
- HollandOnline
- LowLands
- AlbertHeijn
- The Flying Dutchmen
- HellsGate
- VitaminStore
- Chiquita
- SalmPepper
- Supertrips

IDENTIFIED BUYERS

- duhg*** from 's-Gravenpolder
- elme**** from Helmond
- Mind***** from Barneveld
- lg_s**** from Ede
- Ap35* from Zierkzee
- Rams** from Enschede
- JJva***** from Hengelo
- mfor***** from Leusden
- gang***** from Amerfoort
- Klaa***** from Rotterdam

Figure B.20: Hidden service of the Police and the Judicial Authorities of the Netherlands where usernames of Hansa Market vendors and buyers are published

Abbreviations

3PL	Third Party Logistics
AVS	Address Verification System
ABGB	Allgemeines Bürgerliches Gesetzbuch (<i>engl.</i> : Austrian Civil Code)
B2B	Business-to-Business
B2C	Business-to-Consumer
B2G	Business-to-Government
C2B	Consumer-to-Business
C2C	Consumer-to-Consumer
C2G	Citizen-to-Government
CaaS	Crime-as-a-Service
CAPTCHA	Completely Automated Public Turing test to tell Computers and Humans Apart
CGN	Carrier-grade network address translation
DDoS attack	Distributed Denial-of-Service attack
G2B	Government-to-Business
G2C	Government-to-Citizen
G2G	Government-to-Government
I2P	Invisible Internet Project
ID	Identity Document
IP	Internet Protocol
IRC	Internet Relay Chat
LSP	Logistics Service Provider
P2P	Peer-to-Peer
PCI DSS	Payment Card Industry Data Security Standard
PGP	Pretty Good Privacy
POD	Proof of Delivery
PSP	Payment Service Provider

C. ABBREVIATIONS

ROI	Return on Investment
SEPA	Single Euro Payments Area
StGB	Strafgesetzbuch (<i>engl.</i> : Austrian Criminal Code)
TAN	Transaction Authentication Number
URL	Uniform Resource Locator
VPN	Virtual Private Network

List of Figures

2.1	E-commerce framework	10
2.2	Schematic illustration of an e-commerce transaction	16
3.1	Timing and order of the e-commerce transaction processes	31
7.1	Range of cybercrime	102
7.2	Europol's Cybercrime Trichotomy	103
7.3	Schematic illustration of a proxy server	111
7.4	Schematic illustration of a VPN	112
7.5	Schematic illustration of an anonymising network	114
8.1	Schematic illustration of the scale of the Surface Web, the Deep Web and the Darknet	134
8.2	Explorative approach for discovering hidden services in the Darknet	136

List of Tables

2.1	Global B2C e-commerce figures (2015)	11
2.2	Categories of e-commerce	12
2.3	Top five online payment methods in 2014, 2015, and 2020 (forecast)	17
3.1	Evaluation of online payment methods	36
3.2	Evaluation of the risk potential of delivery vulnerabilities	40
5.1	Accuracy rates of a fraud detection system	58
7.1	Commonly used messaging services used by cybercriminals of certain language groups in 2016	118

Bibliography

- [1] Statistik Austria. *IKT-Einsatz in Haushalten*. http://www.statistik.at/web_de/statistiken/energie_umwelt_innovation_mobilitaet/informationsgesellschaft/ikt-einsatz_in_haushalten/index.html. Accessed: 2016-02-04.
- [2] Ecommerce Foundation. *Global B2C Ecommerce Report 2016*. 2016. https://www.ecommercewiki.org/Prot:Global_B2C_Ecommerce_Report_2016. Accessed: 2017-03-24.
- [3] statista. *Prognose zur Anzahl der E-Commerce-Nutzer weltweit in den Jahren 2015 bis 2021*. <https://de.statista.com/statistik/daten/studie/485005/umfrage/prognose-der-e-commerce-nutzer-weltweit/>. Accessed: 2016-12-13.
- [4] PYMNTS/Forster. *Global fraud attack index Q4 2016*. <http://pymnts.fetchapp.com/files/c67569>. Accessed: 2016-01-09.
- [5] CRIF. *CRIF Umfrage: Betrug im Online-Handel nimmt zu*. 2017. <https://www.crif.at/pr-events/pressemeldungen/2017/mai/05/crif-umfrage-betrug-im-online-handel-nimmt-zu/>. Accessed: 2017-05-06.
- [6] Rippleshot. *2016 Trends in global eCommerce Fraud*. 2016. <http://info.rippleshot.com/blog/2016-trends-in-global-ecommerce-fraud>. Accessed: 2016-01-09.
- [7] Rentian Huang, Hissam Tawfik, and Atulya Nagar. "Towards an artificial immune system for online fraud detection". In: *International Conference on Artificial Immune Systems*. Springer. 2011, pp. 383–394.
- [8] Europol. *The Internet Organised Crime Threat Assessment (iOCTA) 2016*. Europol, 2016.
- [9] Derek Manky. "Cybercrime as a service: a very modern business". In: *Computer Fraud & Security* 2013.6 (2013), pp. 9–13. ISSN: 1361-3723.
- [10] David Tait. *Cybercrime: Innovative approaches to an unprecedented challenge*. 2015. <http://www.commonwealthgovernance.org/assets/uploads/2015/04/CGH-15-Tait.pdf>. Accessed: 2017-01-28.

- [11] Europol. *The Internet Organised Crime Threat Assessment (iOCTA) 2015*. Europol, 2015.
- [12] ibi research GmbH. *Betrug und Betrugsprävention im Online-Handel*. 2015. <https://ecommerce-leitfaden.de/studien/item/betrug-und-betrugspraevention-im-online-handel>. Accessed: 2016-12-14.
- [13] Megan F Hess and James H Cottrell. “Fraud risk management: A small business perspective”. In: *Business Horizons* 59.1 (2016), pp. 13–18.
- [14] Oxford Dictionaries. *Definition of commerce*. <https://en.oxforddictionaries.com/definition/commerce>. Accessed: 2017-01-24.
- [15] Rolf T Wigand. “Electronic commerce: Definition, theory, and context”. In: *The information society* 13.1 (1997), pp. 1–16.
- [16] Soon-Yong Choi, Dale O Stahl, and Andrew B Whinston. *The economics of electronic commerce*. Macmillan Technical Publishing Indianapolis, IN, 1997.
- [17] S. Madan. *Securing Transactions and Payment Systems for M-Commerce*. Advances in E-Business Research. IGI Global, 2016.
- [18] A. Manzoor. *E-Commerce: An Introduction*. Lambert Academic Publishing, 2010.
- [19] statista. *E-commerce share of total global retail sales from 2015 to 2020*. <https://www.statista.com/statistics/534123/e-commerce-share-of-retail-sales-worldwide/>. Accessed: 2017-03-20.
- [20] Dave Chaffey. *E-business and E-commerce Management: Strategy, Implementation and Practice*. Pearson Education, 2007.
- [21] Gary P. Schneider. *Electronic Commerce*. Cengage Learning, 2015.
- [22] Efraim Turban et al. *Electronic commerce: A managerial and social networks perspective*. Springer, 2015.
- [23] Zheng Qin. *Introduction to E-commerce*. Tsinghua University texts. Springer Berlin Heidelberg, 2010.
- [24] Dhiraj Sharma. *Foundations of IT*. Excel Books, 2009.
- [25] Chiel Liezenberg, Douwe Lycklama, and Harry Smorenberg. “Understanding buyer and seller behaviour for improved payment product development”. In: *Journal of Payments Strategy & Systems* 1.3 (2007), pp. 219–227.
- [26] Pita Jarupunphol and Chris J Mitchell. “Measuring 3-D Secure and 3D SET against e-commerce end-user requirements”. In: *Proceedings of the 8th Collaborative Electronic Commerce Technology and Research Conference*. Citeseer. 2003, pp. 51–64.
- [27] Nucharee Premchaiswadi, James G Williams, and Wichian Premchaiswadi. “A Study of an On-Line Credit Card Payment Processing and Fraud Prevention for e-Business”. In: *E-Learn: World Conference on E-Learning in Corporate, Government, Healthcare, and Higher Education*. Vol. 2009. 1. 2009, pp. 2199–2206.

-
- [28] V. Hassler and P. Moore. *Security Fundamentals for E-commerce*. Artech House computer security series: New series. Artech House, 2001.
- [29] The Paypers. *Ecommerce Payment Methods Report 2016*. 2016. <http://www.thepappers.com/reports/ecommerce-payment-methods-report-2016-global-payments-insights/r765256>. Accessed: 2017-03-28.
- [30] D.A. Montague. *Essentials of Online payment Security and Fraud Prevention*. Essentials Series. Wiley, 2010.
- [31] Hanna Wolsfelt. *Merchant Account vs. Payment Gateway: What's the Difference?* <https://home.bluesnap.com/snap-center/blog/merchant-account-vs-payment-gateway/>. Accessed: 2017-03-29.
- [32] Catalin Zorzini. *What is the Difference Between a Payment Processor, Payment Gateway, and a Merchant Account?* 2017. <http://ecommerce-platforms.com/ecommerce-selling-advice/what-is-difference-between-a-payment-gateway-payment-processor-and-a-merchant-account>. Accessed: 2017-03-29.
- [33] Bob Travica. “Think process, think in time: advancing study of informing systems”. In: *Informing Science: the International Journal of an Emerging Transdiscipline* 17 (2014), pp. 133–149.
- [34] Jay Joong-Kun Cho, John Ozment, and Harry Sink. “Logistics capability, logistics outsourcing and firm performance in an e-commerce market”. In: *International journal of physical distribution & logistics management* 38.5 (2008), pp. 336–359.
- [35] Elliot Rabinovich, A Michael Knemeyer, and Chad M Mayer. “Why do Internet commerce firms incorporate logistics service providers in their distribution channels?: The role of transaction costs and network strength”. In: *Journal of Operations Management* 25.3 (2007), pp. 661–681.
- [36] Werner Delfmann, Sascha Albers, and Martin Gehring. “The impact of electronic commerce on logistics service providers”. In: *International Journal of Physical Distribution & Logistics Management* 32.3 (2002), pp. 203–222.
- [37] Sandra Wróbel-Konior. *Online Payments in A Nutshell: A Guide for Beginners*. <https://securionpay.com/blog/online-payments-nutshell-guide-e-beginners/>. Accessed: 2017-04-04.
- [38] worldpay. *Global Payments Report 2015*. 2016. <http://offers.worldpayglobal.com/rs/850-JOA-856/images/GlobalPaymentsReportNov2015.pdf>. Accessed: 2017-04-05.
- [39] worldpay. *Global Payments Report 2016*. 2016. <https://worldpay.globalpaymentsreport.com/introduction/>. Accessed: 2017-03-28.
- [40] Numen - The Latin Lexicon. *Definition of fraus*. <http://latinlexicon.org/definition.php?p1=1006487>. Accessed: 2017-02-21.

- [41] Bundeskanzleramt. *Bundesrecht konsolidiert: Gesamte Rechtsvorschrift für Strafgesetzbuch, Fassung vom 20.02.2017*. <https://www.ris.bka.gv.at/Gelten.deFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10002296>. Accessed: 2017-02-20.
- [42] Frank Höpfel Andreas Schloenhardt. *Strafgesetzbuch / Austrian Criminal Code*. Ed. by Frank Höpfel Andreas Schloenhardt. NWV Verlag, 2016.
- [43] Pattama Malakedsuwan and Kenneth Stevens. “A Model of E-Fraud”. In: *PACIS 2003 Proceedings* (2003), p. 2.
- [44] BusinessDictionary. *Fraud (Definition)*. <http://www.businessdictionary.com/definition/fraud.html>. Accessed: 2017-02-20.
- [45] Jovan Kurbalija. *An Introduction to Internet Governance*. DiploFoundation, 2016.
- [46] Europol. *Situation Report - Payment Card Fraud in the European Union*. 2012. <https://www.europol.europa.eu/publications-documents/situation-report-payment-card-fraud-in-european-union>. Accessed: 2017-04-07.
- [47] Priya J Rana and Jwalant Baria. “A Survey on Fraud Detection Techniques in Ecommerce”. In: *International Journal of Computer Applications* 113.14 (2015).
- [48] Siddhartha Bhattacharyya et al. “Data mining for credit card fraud: A comparative study”. In: *Decision Support Systems* 50.3 (2011), pp. 602–613.
- [49] Gareth Jones. “E-commerce and identity fraud”. In: *Interactive Marketing* 2.4 (2001), pp. 357–372.
- [50] Europol. *The Internet Organised Crime Threat Assessment (iOCTA) 2014*. Europol, 2014.
- [51] Shuang Hao et al. “Drops for stuff: An analysis of reshipping mule scams”. In: *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*. ACM. 2015, pp. 1081–1092.
- [52] Europol. *European Union Serious and Organised Crime Threat Assessment 2017*. Europol, 2017.
- [53] C Richard Baker. “Crime, fraud and deceit on the internet: is there hyperreality in cyberspace?” In: *Critical Perspectives on Accounting* 13.1 (2002), pp. 1–15.
- [54] Chioma Vivian Amasiatu and Mahmood Hussain Shah. “First party fraud: a review of the forms and motives of fraudulent consumer behaviours in e-tailing”. In: *International Journal of Retail & Distribution Management* 42.9 (2014), pp. 805–817.
- [55] Verifi. *What every card not present merchant should know*. 2014. http://www.verifi.com/wp-content/uploads/2014/05/Verifi_eBook_web_noCNP.pdf. Accessed: 2017-01-19.

-
- [56] Janna Leyde. *The Guide to E-Commerce Fraud*. 2014. https://www.2checkout.com/upload/documents/ebook_Guide_to_Ecommerce_Fraud.pdf. Accessed: 2017-03-02.
- [57] Richard J Sullivan. “Controlling security risk and fraud in payment systems”. In: *Economic Review-Federal Reserve Bank of Kansas City* (2014), p. 5.
- [58] U.S. Payments Forum. *Card-Not-Present Fraud around the World*. 2017. <http://www.uspaymentsforum.org/cnp-fraud-around-the-world/>. Accessed: 2017-04-16.
- [59] No author. “43% of credit card fraud not reported”. In: *Network Security* 2000.10 (2000), p. 4.
- [60] David J Hand and David J Weston. “Statistical techniques for fraud detection, prevention, and assessment”. In: *Mining massive data sets for security* (2008), pp. 257–270.
- [61] Association for Financial Professionals (AFP). *2016 AFP Payments Fraud and Control Survey*. 2016. <https://www.afponline.org/publications-data-tools/reports/survey-research-economic-data/Details/payments-fraud-2016>. Accessed: 2017-05-17.
- [62] LexisNexis. *2016 True Cost of Fraud Study*. 2016. <http://www.lexisnexis.com/risk/insights/true-cost-fraud.aspx>. Accessed: 2017-01-09.
- [63] Tej Paul Bhatla, Vikram Prabhu, and Amit Dua. “Understanding credit card frauds”. In: *Cards business review* 1.6 (2003).
- [64] Jon TS Quah and M Sriganesh. “Real-time credit card fraud detection using computational intelligence”. In: *Expert systems with applications* 35.4 (2008), pp. 1721–1732.
- [65] Theresa Ward. “Strategies for Reducing the Risk of eCommerce Fraud”. In: *Atlanta: First Data Corporation* (2010).
- [66] Chargebacks911. *Best Indicators of Fraud for Card-Not-Present Transactions*. <https://chargebacks911.com/knowledge-base/best-indicators-of-fraud-for-card-not-present-transactions/>. Accessed: 2017-05-09.
- [67] Ben Dwyer. *Chargebacks: A Survival Guide*. <https://www.cardfellow.com/chargebacks/>. Accessed: 2017-04-14.
- [68] Smart Card Alliance. *Card-Not-Present Fraud: A Primer on Trends and Authentication Processes*. 2014. <http://www.smartcardalliance.org/resources/pdf/CNP-WP-FINAL-022114.pdf>. Accessed: 2017-01-22.
- [69] Bundeskanzleramt. *Bundesrecht konsolidiert: Allgemeines bürgerliches Gesetzbuch § 870, Fassung vom 10.05.2017*. <https://www.ris.bka.gv.at/Gelten.deFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10001622>. Accessed: 2017-05-10.

- [70] Achmad Nizar Hidayanto, Hamzah Saifulhaq, and Putu Wuri Handayani. "Do consumers really care on risks in online shopping? An analysis from Indonesian online consumers". In: *2012 IEEE International Conference on Management of Innovation and Technology (ICMIT)*. IEEE. 2012, pp. 331–336.
- [71] Anne-Sophie Cases. "Perceived risk and risk-reduction strategies in Internet shopping". In: *The International Review of Retail, Distribution and Consumer Research* 12.4 (2002), pp. 375–394.
- [72] Xueming Luo. "Trust production and privacy concerns on the Internet: A framework based on relationship marketing and social exchange theory". In: *Industrial Marketing Management* 31.2 (2002), pp. 111–118.
- [73] Khyati Chaudhary and Bhawna Mallick. "Credit Card Fraud: Bang in E-Commerce". In: *Editorial Board* (2012), p. 935.
- [74] Oleg Victorovich Sobko. "Fraud in Non-Cash Transactions: Methods, Tendencies and Threats". In: *World Applied Sciences Journal* 29.6 (2014), pp. 774–778.
- [75] G. Borges et al. *Identitätsdiebstahl und Identitätsmissbrauch im Internet: Rechtliche und technische Aspekte*. Springer Berlin Heidelberg, 2011.
- [76] Bert-Jaap Koops and Ronald Leenes. "Identity theft, identity fraud and/or identity-related crime". In: *Datenschutz und Datensicherheit-DuD* 30.9 (2006), pp. 553–556.
- [77] Umesh Shankar and Miriam Walker. "A survey of security in online credit card payments". In: *policy* 6 (2001), p. 7.
- [78] Justin Pritchard. *Tips for Using a Debit Card Online*. 2017. <https://www.thebalance.com/can-i-use-a-debit-card-online-315325>. Accessed: 2017-04-21.
- [79] Chargebacks911. *How do Credit Card and Debit Card Chargebacks Differ?* 2015. <https://chargebacks911.com/debit-card-chargeback/>. Accessed: 2017-04-21.
- [80] Riccardo Mangiaracina and Alessandro Perego. "Payment systems in the B2c eCommerce: Are they a barrier for the online customer?" In: *Journal of Internet Banking and Commerce* 14.3 (2009), p. 1.
- [81] PayPal. *Purchase protection you need, peace of mind you deserve*. <https://www.paypal.com/us/webapps/mpp/paypal-safety-and-security>. Accessed: 2017-04-20.
- [82] PayPal. *Seller Protection for Merchants*. <https://www.paypal.com/us/webapps/mpp/security/seller-protection>. Accessed: 2017-04-20.
- [83] Alan C McKinnon and Deepak Tallam. "Unattended delivery to the home: an assessment of the security implications". In: *International Journal of Retail & Distribution Management* 31.1 (2003), pp. 30–41.
- [84] Mark Xu, Brett Ferrand, and Martyn Roberts. "The last mile of e-commerce—unattended delivery from the consumers and eTailers' perspectives". In: *International Journal of Electronic Marketing and Retailing* 2.1 (2008), pp. 20–38.

-
- [85] John Fernie and AC McKinnon. “The development of e-tail logistics”. In: *Logistics and Retail Management, 2nd edition, Kogan Page, London* (2004), pp. 164–187.
- [86] Alan McKinnon and Deepak Tallam. “New crime threats from e-tailing: theft in the home delivery channel”. In: *report prepared for the Products and Crime Task Force of the UK Government Foresight Programme, UK Government, London* (2002).
- [87] DHL. *Pakete an einer DHL Packstation empfangen*. <https://www.dhlpaket.at/de/privatkunden/pakete-empfangen/packstation.html>. Accessed: 2017-05-06.
- [88] Jesse WJ Weltevreden. “B2c e-commerce logistics: the rise of collection-and-delivery points in The Netherlands”. In: *International Journal of Retail & Distribution Management* 36.8 (2008), pp. 638–660.
- [89] DHL. *Ident-check*. <https://www.dhl.de/en/paket/information/geschaeftskunden/service-ident-check.html>. Accessed: 2017-05-16.
- [90] DPD. *ID-Check for the Express-Service*. https://www.dpd.com/de_en/sending_parcel/our_options. Accessed: 2017-05-16.
- [91] Karisse Hendrick. *Parcel Forwarding: Fly-By-Night or Totally Right?* <https://cardnotpresent.com/parcel-forwarding-fly-by-night-or-totally-right/>. Accessed: 2017-05-16.
- [92] Kevin Woodward. *E-Retailers Take Heed: Certain ZIP Codes Harbor a Lot More Fraud Than Others*. http://www.digitaltransactions.net/news/story/E-Retailers-Take-Heed_-Certain-ZIP-Codes-Harbor-a-Lot-More-Fraud-Than-Others. Accessed: 2017-05-16.
- [93] Raymond Rau. *What does a freight forwarder do & do you need one?* 2014. <http://www.universalcargo.com/what-does-a-freight-forwarder-do-do-you-need-one/>. Accessed: 2017-05-16.
- [94] Visa. *Visa E-Commerce Merchants’ Guide to Risk Management*. 2013. <https://usa.visa.com/dam/VCOM/download/merchants/visa-risk-management-guide-ecommerce.pdf>. Accessed: 2017-05-09.
- [95] John R. Vacca. *Identity Theft*. Prentice Hall Professional, 2003.
- [96] Yarden Altshull. *Package Rerouting: Managing the Risk Factor*. 2016. <https://blog.riskified.com/package-rerouting-managing-the-risk-factor/>. Accessed: 2017-05-16.
- [97] W.S. Albrecht et al. *Fraud Examination*. Cengage Learning, 2011.
- [98] Sharon Curry. *An Inside Look at E-Commerce Fraud*. 2000. <https://www.scambusters.org/ecommercefraud.pdf>. Accessed: 2017-05-07.
- [99] Frank S Perri. “White-Collar Criminals: The ‘Kinder, Gentler’ Offender?” In: *Journal of Investigative Psychology and Offender Profiling* 8.3 (2011), pp. 217–241.

- [100] UniBul's Money Blog. *12 Signs of E-Commerce Fraud*. <http://blog.unibulmerchantservices.com/12-signs-of-e-commerce-fraud/>. Accessed: 2017-01-09.
- [101] Informatics, Inc. *e-Commerce Fraud Prevention - Part 2*. <http://www.informaticsync.com/Blog/20130501/29/e-Commerce-Fraud-Prevention-Part-2.aspx>. Accessed: 2017-05-16.
- [102] TSYS. *Tips for Preventing Credit Card Fraud and Avoiding Chargebacks (White Paper)*. 2017. http://www.tsys.com/Assets/TSYS/downloads/merchant/whitepaper/wp_tips-for-preventing-credit-card-fraud.pdf. Accessed: 2017-07-18.
- [103] Isaac Thuku. *What Tell Tale Signs to look for in E-Commerce Fraud*. <https://www.kenyapesa.com/Resources/What-Tell-Tale-Signs-to-look-for-in-eCommerce-Fraud.php>. Accessed: 2017-05-09.
- [104] sift science. *Signs of Fraud in Shipping Addresses*. <https://siftscience.com/sift-edu/prevent-fraud/signs-fraud-shipping>. Accessed: 2017-05-09.
- [105] Richard J Bolton, David J Hand, et al. "Unsupervised profiling methods for fraud detection". In: *Credit Scoring and Credit Control VII* (2001), pp. 235–255.
- [106] Richard J Bolton and David J Hand. "Statistical fraud detection: A review". In: *Statistical science* (2002), pp. 235–249.
- [107] Yusuf Sahin and Ekrem Duman. "Detecting credit card fraud by ANN and logistic regression". In: *Innovations in Intelligent Systems and Applications (INISTA), 2011 International Symposium on*. IEEE. 2011, pp. 315–319.
- [108] Elli Bishop. *Stop Ecommerce Fraud in Its Tracks: Arm Your Business with These 10 Practices*. <https://blog.kissmetrics.com/stop-ecommerce-fraud/>. Accessed: 2017-05-21.
- [109] John Johansen. *Stop, Thief! 7 Tips To Fight eCommerce Fraud*. <https://home.bluesnap.com/snap-center/blog/stop-thief-7-tips-to-fight-ecommerce-fraud/>. Accessed: 2017-01-09.
- [110] Keith Wong et al. "An Online Audit Review System for Electronic Commerce". In: *Proceedings of the 13th Bled Electronic Commerce Conference*. 2000, pp. 20–23.
- [111] CJ Gahan. "URU—on-line identity verification". In: *BT Technology Journal* 22.1 (2004), pp. 43–51.
- [112] worldpay. *Fraud Trends 2016*. 2016. <http://www.worldpay.com/sites/default/files/Fraud-trends-2016.PDF>. Accessed: 2016-12-14.
- [113] The Fraud Practice. *Manual review technique overview*. <http://www.fraudpractice.com/gl-manual.html>. Accessed: 2017-05-23.
- [114] The Fraud Practice. *Reverse phone number/address checks technique overview*. <http://www.fraudpractice.com/gl-reversephone.html>. Accessed: 2017-05-23.

-
- [115] Trulioo. *Because Knowing Your Customer is Crucial*. <https://www.trulioo.com/>. Accessed: 2017-05-23.
- [116] LexisNexis. *Identity Verification*. <http://www.lexisnexis.com/risk/identity/verification.aspx>. Accessed: 2017-05-23.
- [117] EVS. *Know Who You Are Doing Business With*. <https://www.electronicverificationsystems.com/identity-verification>. Accessed: 2017-05-23.
- [118] TrustID. *For fast, accurate and auditable validation of documents used to support identity*. <https://www.trustid.co.uk/how-identity-scanning-works>. Accessed: 2017-05-22.
- [119] experian. *Seamless ID document verification*. <http://www.experian.co.uk/identity-and-fraud/identity-checking/photo-id-validation.html>. Accessed: 2017-05-22.
- [120] Trulioo. *ID Document Verification*. <https://www.trulioo.com/product/id-document-verification/>. Accessed: 2017-05-23.
- [121] IDnow. *IDnow Video-Ident: AML solution for online identification via video chat*. <https://www.idnow.eu/products/video-ident>. Accessed: 2017-05-22.
- [122] Deutsche Post AG. *POSTIDENT via video chat*. <https://www.deutschepost.de/en/p/postident/identifizierungsverfahren/verfahren-videochat.html>. Accessed: 2017-05-22.
- [123] Deutsche Post AG. *An overview of the POSTIDENT process*. <https://www.deutschepost.de/en/p/postident/identifizierungsverfahren.html>. Accessed: 2017-05-22.
- [124] buergerkarte.at. *Aktivieren der Handy-Signatur*. <https://www.buergerkarte.at/aktivieren-handy.html>. Accessed: 2017-05-22.
- [125] Danny Bluestone. *Key trends in online identity verification (so everybody knows you're a dog)*. <https://econsultancy.com/blog/67718-key-trends-in-online-identity-verification-so-everybody-knows-you-re-a-dog/>. Accessed: 2017-05-22.
- [126] buergerkarte.at. *Das kann die Bürgerkarte*. <https://www.buergerkarte.at/anwendungen-karte.html>. Accessed: 2017-05-22.
- [127] Bundeskanzleramt. *Handy-Signatur*. <https://www.help.gv.at/Portal.Node/hlpd/public/content/221/Seite.2210002.html>. Accessed: 2017-05-22.
- [128] GOV.UK. *Guidance GOV.UK Verify*. <http://www.telegraph.co.uk/technology/news/11150072/How-the-government-plans-to-verify-your-identity-online.html>. Accessed: 2017-05-22.
- [129] AfterPay. *Pay after delivery*. <https://www.afterpay.nl/en/business-partners-afterpay/why-afterpay>. Accessed: 2017-05-28.

- [130] payolution. *payment by invoice*. <https://www.payolution.com/en/products/invoice/>. Accessed: 2017-05-28.
- [131] PCI Compliance Guide. *What is PCI?* <https://www.pcicomplianceguide.org/pci-faqs-2/#1>. Accessed: 2017-05-28.
- [132] PCI Security Standards Council LLC. *PCI Data Storage Do's and Don'ts*. https://www.pcisecuritystandards.org/pdfs/pci_fs_data_storage.pdf. Accessed: 2017-05-28.
- [133] Vanesa Gil Laredo. "PCI DSS compliance: a matter of strategy". In: *Card Technology Today* 20.4 (2008), p. 9.
- [134] Steve Lomax. "Securing the eCommerce revolution: safeguarding Internet transactions". In: *Card Technology Today* 18.6 (2006), pp. 9–10.
- [135] Markus Ruch and Stefan Sackmann. "Customer-specific transaction risk management in e-commerce". In: *Value Creation in E-Business Management*. Springer, 2009, pp. 68–79.
- [136] Stefan Weinfurtner et al. "Erfolgsfaktor Payment—Der Einfluss der Zahlungsverfahren auf Ihren Umsatz". In: *Aktuelle Ergebnisse zum Bezahlverhalten der Endkunden aus dem Projekt E-Commerce-Leitfaden, 2nd edition, ibi research, Regensburg* (2013).
- [137] Eleonora Morganti et al. "The impact of e-commerce on final deliveries: alternative parcel delivery services in France and Germany". In: *Transportation Research Procedia* 4 (2014), pp. 178–190.
- [138] AS Bekirev et al. "Payment card fraud detection using neural network committee and clustering". In: *Optical Memory and Neural Networks* 24.3 (2015), pp. 193–200.
- [139] Daniel Sánchez et al. "Association rules applied to credit card fraud detection". In: *Expert systems with applications* 36.2 (2009), pp. 3630–3640.
- [140] Ekrem Duman and M Hamdi Ozcelik. "Detecting credit card fraud by genetic algorithm and scatter search". In: *Expert Systems with Applications* 38.10 (2011), pp. 13057–13063.
- [141] M Krivko. "A hybrid model for plastic card fraud detection systems". In: *Expert Systems with Applications* 37.8 (2010), pp. 6070–6076.
- [142] Yufeng Kou et al. "Survey of fraud detection techniques". In: *IEEE international conference on Networking, Sensing and Control, 2004*. Vol. 2. IEEE. 2004, pp. 749–754.
- [143] Tanmay Kumar Behera and Suvasini Panigrahi. "Credit Card Fraud Detection: A Hybrid Approach Using Fuzzy Clustering & Neural Network". In: *Second International Conference on Advances in Computing and Communication Engineering (ICACCE), 2015*. IEEE. 2015, pp. 494–499.
- [144] Suvasini Panigrahi et al. "Credit card fraud detection: A fusion approach using Dempster-Shafer theory and Bayesian learning". In: *Information Fusion* 10.4 (2009), pp. 354–363.

-
- [145] Tom Fawcett and Foster Provost. “Adaptive fraud detection”. In: *Data mining and knowledge discovery* 1.3 (1997), pp. 291–316.
- [146] Clifton Phua et al. “A comprehensive survey of data mining-based fraud detection research”. In: *arXiv preprint arXiv:1009.6119* (2010).
- [147] Vishal Vatsa, Shamik Sural, and Arun K Majumdar. “A game-theoretic approach to credit card fraud detection”. In: *International Conference on Information Systems Security*. Springer. 2005, pp. 263–276.
- [148] Robert Nisbet, John Elder, and Gary Miner. “Chapter 17 - Fraud Detection”. In: *Handbook of Statistical Analysis and Data Mining Applications*. Ed. by Robert Nisbet, John Elder, and Gary Miner. Boston: Academic Press, 2009, pp. 347–361. ISBN: 978-0-12-374765-5.
- [149] Rong-Chang Chen et al. “Detecting credit card fraud by using questionnaire-responded transaction model based on support vector machines”. In: *Intelligent Data Engineering and Automated Learning-IDEAL 2004* (2004), pp. 800–806.
- [150] Jose R Dorronsoro et al. “Neural fraud detection in credit card operations”. In: *IEEE transactions on neural networks* 8.4 (1997), pp. 827–834.
- [151] Foster Provost. “[Statistical Fraud Detection: A Review]: Comment”. In: *Statistical Science* 17.3 (2002), pp. 249–251.
- [152] Mohammad Behdad et al. “On XCSR for electronic fraud detection”. In: *Evolutionary Intelligence* 5.2 (2012), pp. 139–150.
- [153] Jarrod West and Maumita Bhattacharya. “Intelligent financial fraud detection: a comprehensive review”. In: *Computers & Security* 57 (2016), pp. 47–66.
- [154] Abhinav Srivastava et al. “Credit card fraud detection using hidden Markov model”. In: *IEEE Transactions on dependable and secure computing* 5.1 (2008), pp. 37–48.
- [155] Seonyoung Shim and Byungtae Lee. “An economic model of optimal fraud control and the aftermarket for security services in online marketplaces”. In: *Electronic Commerce Research and Applications* 9.5 (2010), pp. 435–445.
- [156] Paul Fichtman. “Preventing Credit Card Fraud and Identity Theft: A Primer for Online Merchants”. In: *Information Systems Security* 10.5 (2001), pp. 1–8.
- [157] S Dejan. “Reducing fraud in electronic payment systems”. In: *The 7th Balkan Conference on Operational Research, BACOR*. Vol. 5. 2005, pp. 1–11.
- [158] Linda Delamaire, HAH Abdou, and John Pointon. “Credit card fraud and detection techniques: a review”. In: *Banks and Bank systems* 4.2 (2009), pp. 57–68.
- [159] Mark Button. “Cross-border fraud and the case for an “Interfraud””. In: *Policing: An International Journal of Police Strategies & Management* 35.2 (2012), pp. 285–303.

- [160] EHI Retail Institute GmbH. *Informationen zu KUNO*. <https://www.kuno-sperrendienst.de/index.cfm?fuseaction=public.displayAboutKUNO>. Accessed: 2017-06-12.
- [161] SCHUFA. *SCHUFA-FraudPool*. <https://www.schufa.de/de/unternehmenskunden/leistungen/fraudprevention-compliance/schufa-fraudpool/>. Accessed: 2017-06-12.
- [162] Constantinos S Hilas. “Designing an expert system for fraud detection in private telecommunications networks”. In: *Expert Systems with applications* 36.9 (2009), pp. 11559–11569.
- [163] Shu-Hsien Liao. “Expert system methodologies and applications—a decade review from 1995 to 2004”. In: *Expert systems with applications* 28.1 (2005), pp. 93–103.
- [164] Michael Sternberg and Robert G. Reynolds. “Using cultural algorithms to support re-engineering of rule-based expert systems in dynamic performance environments: a case study in fraud detection”. In: *IEEE Transactions on Evolutionary Computation* 1.4 (1997), pp. 225–243.
- [165] Naeimeh Laleh and Mohammad Abdollahi Azgomi. “A taxonomy of frauds and fraud detection techniques”. In: *International Conference on Information Systems, Technology and Management*. Springer. 2009, pp. 256–267.
- [166] K. K. Sherly. “A comparative assessment of supervised data mining techniques for fraud prevention”. In: *International Journal of Science and Technology Research* 1.16 (2012).
- [167] Aihua Shen, Rencheng Tong, and Yaochen Deng. “Application of classification models on credit card fraud detection”. In: *International Conference on Service Systems and Service Management, 2007*. IEEE. 2007, pp. 1–4.
- [168] Richard Wheeler and Stuart Aitken. “Multiple algorithms for fraud detection”. In: *Knowledge-Based Systems* 13.2 (2000), pp. 93–99.
- [169] Masoumeh Zareapoor, KR Seeja, and M Afshar Alam. “Analysis on Credit Card Fraud Detection Techniques: Based on Certain Design Criteria”. In: *International Journal of Computer Applications* 52.3 (2012).
- [170] Raghavendra Patidar, Lokesh Sharma, et al. “Credit card fraud detection using neural network”. In: *International Journal of Soft Computing and Engineering (IJSCE)* 1.32-38 (2011).
- [171] S Benson Edwin Raj and A Annie Portia. “Analysis on credit card fraud detection methods”. In: *International Conference on Computer, Communication and Electrical Technology (ICCCET), 2011*. IEEE. 2011, pp. 152–156.
- [172] Sam Maes et al. “Credit card fraud detection using Bayesian and neural networks”. In: *Proceedings of the 1st international naiso congress on neuro fuzzy technologies*. 2002, pp. 261–270.
- [173] Nuno Carneiro, Gonçalo Figueira, and Miguel Costa. “A data mining based system for credit-card fraud detection in e-tail”. In: *Decision Support Systems* (2017).

- [174] Larry Bull. “Learning classifier systems: A brief introduction”. In: *Applications of Learning Classifier Systems*. Springer, 2004, pp. 1–12.
- [175] Jürgen Branke. “Brief Introduction to Evolutionary Algorithms”. In: *Evolutionary Optimization in Dynamic Environments* (2002), pp. 1–10.
- [176] Khyati Chaudhary, Jyoti Yadav, and Bhawna Mallick. “A review of fraud detection techniques: Credit card”. In: *International Journal of Computer Applications* 45.1 (2012), pp. 39–44.
- [177] James A Tackett and Fran Wolf. “Link analysis for fraud detection”. In: *Journal of Corporate Accounting & Finance* 23.4 (2012), pp. 7–13.
- [178] F Fogelman-Soulié, A Mekki, and S Sean. “Using Social Networks for On-line Credit Card Fraud Analysis”. In: *Use of Risk Analysis in Computer-Aided Persuasion*, editors Ekrem Duman, Amir Atiya Eds, NATO Science for Peace and Security Series, E 88 (2011), pp. 60–72.
- [179] Helmut Koziol, Peter Bydliniski, and Raimund Bollenberger, eds. *Kurzkommentar zum ABGB*. 3rd ed. SpringerWienNewYork, 2010.
- [180] Marc-Philippe Weller. *Die Vertragstreue: Vertragsbindung - Naturalerfüllungsgrundsatz - Leistungstreue*. Jus Privatum Series. Mohr Siebeck, 2009.
- [181] Pircher-Eschig Erika Eschig Peter. *Das österreichische ABGB - The Austrian Civil Code*. LexisNexis, 2013.
- [182] Bundeskanzleramt. *NOR12018593*. 1917. <https://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Bundesnormen&Dokumentnummer=NOR12018593>. Accessed: 2017-06-24.
- [183] Heinz Barta. *Zivilrecht: Grundriss und Einführung in das Rechtsdenken. 1*. WUV- Univ.-Verlag, 2004.
- [184] Christoph Lang. *Arbeitsrechtliche Unterschiede zwischen Deutschland und Österreich*. Salzwasser-Verlag, 2008.
- [185] Johannes Öhlböck. *Betrug | gewerbsmäßiger Betrug | Rechtsanwalt | Strafverfahren / Strafverhandlung*. <http://www.rechtsfreund.at/strafrecht/betrug.htm>. Accessed: 2017-06-21.
- [186] Helmut Fuchs and Susanne Reindl-Krauskopf. *Strafrecht. Besonderer Teil I*. 3rd ed. SpringerWienNewYork, 2009.
- [187] Klaus Schwaighofer Christian Bertel. *Österreichisches Strafrecht - Besonderer Teil 1 (§§ 75 bis 168e StGB)*. 11th ed. Springers Kurzlehrbücher der Rechtswissenschaft, 2010.
- [188] Bundeskanzleramt. *Geschäftszahl 13Os2/07d*. 2007. https://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Justiz&Dokumentnummer=JJT_20070307_OGH0002_01300S00002_07D0000_000. Accessed: 2017-06-21.

- [189] Bundeskanzleramt. *Geschäftszahl 13Os61/11m*. 2011. https://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Justiz&Dokumentnummer=JJT_20110714_OGH0002_01300S00061_11M0000_000. Accessed: 2017-06-21.
- [190] Klaus Schwaighofer Christian Bertel. *Österreichisches Strafrecht - Besonderer Teil 2 (§§ 169 bis 321 StGB)*. Springers Kurzlehrbücher der Rechtswissenschaft, 2010.
- [191] Reformgruppe zum Strafgesetzbuch. *Bericht des Bundesministers für Justiz über die Fortschritte der Reformgruppe zum Strafgesetzbuch (III-104 d.B.)* 2014. https://www.parlament.gv.at/PAKT/VHG/XXV/III/III_00104/imfname_366604.pdf. Accessed: 2017-06-22.
- [192] Susanne Reindl. “Das Phänomen „Phishing“. Aktuelles Computerstrafrecht.” In: *SIAKJournal-Zeitschrift für Polizeiwissenschaft und polizeiliche Praxis* (2007), pp. 2–13.
- [193] Johannes Beer. *Die Convention on Cybercrime und österreichisches Strafrecht*. Schriften der Johannes-Kepler-Universität Linz / A. C. Hofer, 2005.
- [194] Helmut Fuchs. *Österreichisches Strafrecht, Allgemeiner Teil 1; Grundlagen und Lehre von der Straftat*. 7th ed. SpringerWienNewYork, 2008.
- [195] M Brandl. “Zur strafrechtlichen Verantwortung bei der Nutzung des Internets”. In: *e&i Elektrotechnik und Informationstechnik* 120.7-8 (2003), pp. 230–234.
- [196] Thomas J. Primig. *Internationales Strafrecht und das Internet*. 2002. http://www.rechtsprobleme.at/doks/primig-1-internationales_strafrecht.pdf. Accessed: 2017-06-23.
- [197] Clemens Thiele. “Straftaten im Cyberspace–Zur Reichweite des österreichischen internationalen Strafrechts”. In: *Medien und Recht* 4 (1998), pp. 219–226.
- [198] Marco Gercke. “Europe’s legal approaches to cybercrime”. In: *ERA-Forum*. Vol. 10. 3. Springer. 2009, pp. 409–420.
- [199] Council of Europe. *Budapest Convention and related standards*. <https://www.coe.int/en/web/cybercrime/the-budapest-convention>. Accessed: 2017-06-25.
- [200] Danny Bradbury. “When borders collide: legislating against cybercrime”. In: *Computer Fraud & Security* 2012.2 (2012), pp. 11–15.
- [201] Erik O Wennerström. “EU-Legislation and Cybercrime-A Decade of European Legal Developments”. In: (2004).
- [202] Council of Europe. *Details of Treaty No.185*. <http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185>. Accessed: 2017-06-25.
- [203] Council of Europe. *Chart of signatures and ratifications of Treaty 185*. 2017. <http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures>. Accessed: 2017-06-25.

- [204] Council of Europe. *Convention on Cybercrime*. 2001. <http://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561>. Accessed: 2017-06-25.
- [205] Susanne Reindl-Krauskopf. “Cyber-Kriminalität”. In: *ZaöRV* 74 (2014), pp. 563–574.
- [206] Bundeskanzleramt. *134. Bundesgesetz, mit dem das Strafgesetzbuch, die Strafprozessordnung 1975, das Strafvollzugsgesetz, das Suchtmittelgesetz, das Gerichtssorgengesetz, das Waffengesetz 1996, das Fremdenengesetz 1997 und das Telekommunikationsgesetz geändert werden (Strafrechtsänderungsgesetz 2002)*. https://www.ris.bka.gv.at/Dokumente/BgblPdf/2002_134_1/2002_134_1.pdf. Accessed: 2017-06-25.
- [207] Jonathan Clough. “Towards a common identity? The harmonisation of identity theft laws”. In: *Journal of Financial Crime* 22.4 (2015), pp. 492–512.
- [208] Marco Gercke. “10 years Convention on Cybercrime: Achievements and Failures of the Council of Europe’s Instrument in the Fight against Internet-related Crimes”. In: *Computer law review international* 5 (2011), pp. 142–149.
- [209] The Council of the European Union. *2001/413/JHA: Council Framework Decision of 28 May 2001 combating fraud and counterfeiting of non-cash means of payment*. <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32001F0413>. Accessed: 2017-07-01.
- [210] The Council of the European Union. *Non-cash payments — combating fraud and counterfeiting*. <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM:124212>. Accessed: 2017-07-01.
- [211] Christiane Neger. “Der Rahmenbeschluß des Rates zur Bekämpfung von Betrug und Fälschung im Zusammenhang mit unbaren Zahlungsmitteln”. In: *ÖBA* 10 (2009), pp. 673–674.
- [212] M. Sonntag. *Einführung in das Internetrecht: Rechtsgrundlagen für Informatiker (Ausgabe Österreich)*. Linde Lehrbuch. Linde Verlag GmbH, 2014.
- [213] Lyane Sautner. “Neue Straftatbestände zum Schutz unbarer Zahlungsmittel”. In: *Österreichische Richterzeitung* 2 (2004).
- [214] European Commission. *Combating Fraud and Counterfeiting of Non-Cash Means of Payment*. 2016. https://ec.europa.eu/home-affairs/what-is-new/work-in-progress/initiatives/ezmp_intro_en. Accessed: 2017-07-01.
- [215] European Parliament. *Extension of rules on combating fraud & counterfeiting of non-cash means of payments*. 2016. <http://www.europarl.europa.eu/legislative-train/theme-area-of-justice-and-fundamental-rights/file-combating-fraud-counterfeiting-of-non-cash-means-of-payments>. Accessed: 2017-07-01.

- [216] INTERPOL. *Cybercrime*. <https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime>. Accessed: 2017-07-29.
- [217] Sarah Gordon and Richard Ford. “On the definition and classification of cybercrime”. In: *Journal in Computer Virology* 2.1 (2006), pp. 13–20.
- [218] Team Cymru. “Cybercrime: An Epidemic”. In: *Queue* 4.9 (2006), pp. 24–35.
- [219] Frank J. Cilluffo Robert Wainwright. *Responding to Cybercrime at Scale: Operation Avalanche – A Case Study*. 2017. <https://cchs.gwu.edu/sites/cchs.gwu.edu/files/Responding%20to%20Cybercrime%20at%20Scale%20FINAL.pdf>. Accessed: 2017-06-26.
- [220] Ben Chai. “The economics of cybercrime”. In: *Infosecurity* 6.7 (2009), pp. 36–39.
- [221] Leroy Terrelonge. *Cybercrime Economy: An Analysis of Criminal Communications Strategies*. 2017. <https://go.flashpoint-intel.com/docs/Analysis-of-Cybercriminal-Communications-Strategies>. Accessed: 2017-07-18.
- [222] Kim-Kwang Raymond Choo and Russell G Smith. “Criminal exploitation of online systems by organised crime groups”. In: *Asian journal of criminology* 3.1 (2008), pp. 37–59.
- [223] Aditya K Sood and Richard J Enbody. “Crimeware-as-a-service - A survey of commoditized crimeware in the underground market”. In: *International Journal of Critical Infrastructure Protection* 6.1 (2013), pp. 28–38.
- [224] Gunter Ollmann. “Hacking as a service”. In: *Computer Fraud & Security* 2008.12 (2008), pp. 12–15.
- [225] Yuval Ben-Itzhak. “Organised cybercrime and payment cards”. In: *Card Technology Today* 21.2 (2009), pp. 10–11.
- [226] Michelle Castell. “Mitigating online account takeovers: The case for education”. In: *Retail Payments Risk Forum Survey Paper 27* (2013), p. 2015.
- [227] Europol. *Cybercrime Dependencies Map*. <https://www.europol.europa.eu/publications-documents/cybercrime-dependencies-map>. Accessed: 2017-08-01.
- [228] Mahmoud Gad. “Crimeware marketplaces and their facilitating technologies”. In: *Technology Innovation Management Review* 4.11 (2014).
- [229] Erika Kraemer-Mbula, Puay Tang, and Howard Rush. “The cybercrime ecosystem: Online innovation in the shadows?” In: *Technological Forecasting and Social Change* 80.3 (2013), pp. 541–555.
- [230] Yvonne Jewkes and Majid Yar. *Handbook of Internet Crime*. Willan Publishing, 2010.
- [231] Ben Brewster Babak Akhgar, ed. *Combating Cybercrime and Cyberterrorism: Challenges, Trends and Priorities*. Springer, 2016.
- [232] Max Goncharov. “Russian Underground 101”. In: *Trend Micro Incorporated Research Paper* (2012), p. 26.

-
- [233] E. Willems. *Cybergefahr: Wie wir uns gegen Cyber-Crime und Online-Terror wehren können*. Springer Fachmedien Wiesbaden, 2015.
- [234] The Tor Project. *Tor: Overview*. <https://www.torproject.org/about/overview.html.en>. Accessed: 2017-07-22.
- [235] The Invisible Internet Project (I2P). *How does it work?* <https://geti2p.net/en/about/intro>. Accessed: 2017-07-22.
- [236] The Freenet Project Inc. *What is Freenet?* <https://freenetproject.org/pages/about.html>. Accessed: 2017-07-22.
- [237] Daniel Moore and Thomas Rid. “Cryptopolitik and the Darknet”. In: *Survival* 58.1 (2016), pp. 7–38.
- [238] The Tor Project. *Tor hidden services: How do I access hidden services?* <https://www.torproject.org/docs/faq.html.en#AccessHiddenServices>. Accessed: 2017-07-23.
- [239] The Tor Project. *How is Tor different from other proxies?* <https://www.torproject.org/docs/faq.html.en#Torisdifferent>. Accessed: 2017-07-23.
- [240] The Tor Project. *Configuring a Tor relay on Debian/Ubuntu*. <https://www.torproject.org/docs/tor-relay-debian>. Accessed: 2017-07-23.
- [241] David Décary-Hétu Judith Aldridge. *Cryptomarkets: The Darknet As An Online Drug Market Innovation*. 2015. <http://daviddhetu.openum.ca/files/sites/39/2017/04/Nesta-Final-Report.pdf>. Accessed: 2017-05-16.
- [242] The Invisible Internet Project (I2P). *Naming and Addressbook*. <https://geti2p.net/en/docs/naming>. Accessed: 2017-07-23.
- [243] The Invisible Internet Project (I2P). *Whats an "eepsite"?* <https://geti2p.net/el/faq#eepsite>. Accessed: 2017-07-23.
- [244] The Invisible Internet Project (I2P). *A gentle introduction to how I2P works*. <https://geti2p.net/en/docs/how/intro>. Accessed: 2017-07-23.
- [245] The Freenet Project Inc. *How is Freenet different to Tor? Can I access Google/Facebook/etc through Freenet?* <https://freenetproject.org/pages/help.html>.
- [246] Marti Motoyama et al. “An analysis of underground forums”. In: *Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference*. ACM, 2011, pp. 71–80.
- [247] Michael Yip, Craig Webber, and Nigel Shadbolt. “Trust among cybercriminals? Carding forums, uncertainty and implications for policing”. In: *Policing and Society* 23.4 (2013), pp. 516–539.

- [248] E Rutger Leukfeldt, Anita Lavorgna, and Edward R Kleemans. “Organised Cybercrime or Cybercrime that is Organised? An Assessment of the Conceptualisation of Financial Cybercrime as Organised Crime”. In: *European Journal on Criminal Policy and Research* (2016), pp. 1–14.
- [249] ER Leukfeldt. “Cybercrime and social ties”. In: *Trends in organized crime* 17.4 (2014), pp. 231–249.
- [250] E Rutger Leukfeldt, Edward R Kleemans, and Wouter P Stol. “A typology of cybercriminal networks: from low-tech all-rounders to high-tech specialists”. In: *Crime, Law and Social Change* (2016), pp. 1–17.
- [251] Lillian Ablon, Martin C. Libicki, and Andrea A. Golay. *Markets for Cybercrime Tools and Stolen Data: Hackers’ Bazaar*. RAND Corporation, 2014.
- [252] Jonathan Lusthaus. “How organised is organised cybercrime?” In: *Global Crime* 14.1 (2013), pp. 52–60.
- [253] Thomas J Holt. “Examining the forces shaping cybercrime markets online”. In: *Social Science Computer Review* 31.2 (2013), pp. 165–177.
- [254] Flashpoint. *Highlights & Trends in the Deep & Dark Web*. 2016. <http://go.flashpoint-intel.com/docs/Highlights-Trends-in-the-Deep-Dark-Web>. Accessed: 2017-07-19.
- [255] Mary Aiken. *The Cyber Effect: A Pioneering Cyberpsychologist Explains how Human Behavior Changes Online*. Spiegel & Grau, 2017.
- [256] Aaron W Baur et al. “Cryptocurrencies as a disruption? empirical findings on user adoption and future potential of bitcoin and co”. In: *Conference on e-Business, e-Services and e-Society*. Springer. 2015, pp. 63–80.
- [257] Sarah Meiklejohn et al. “A fistful of Bitcoins: characterizing payments among men with no names”. In: *Communications of the ACM* 59.4 (2016), pp. 86–93.
- [258] Danton Bryans. “Bitcoin and Money Laundering: Mining for an Effective Solution”. In: *Indiana Law Journal* 89.1 (2014), p. 13.
- [259] CoinMarketCap. *CryptoCurrency Market Capitalizations - All Currencies*. <https://coinmarketcap.com/currencies/views/all/>. Accessed: 2017-07-20.
- [260] Eurojust / Europol. *Common challenges in combating cybercrime - As identified by Eurojust (EJ) and Europol (EP)*. 2017. <http://data.consilium.europa.eu/doc/document/ST-7021-2017-INIT/en/pdf>. Accessed: 2017-07-10.
- [261] Jordi Herrera-Joancomarti. “Research and Challenges on Bitcoin Anonymity”. In: *Data Privacy Management, Autonomous Spontaneous Security, and Security Assurance*. Springer, 2015, pp. 3–16.
- [262] John Suler. “The online disinhibition effect”. In: *Cyberpsychology & behavior* 7.3 (2004), pp. 321–326.
- [263] John Suler. “The online disinhibition effect”. In: *International Journal of Applied Psychoanalytic Studies* 2.2 (2005), pp. 184–188.

- [264] Cameron SD Brown. “Investigating and prosecuting cyber crime: forensic dependencies and barriers to justice”. In: *International Journal of Cyber Criminology* 9.1 (2015), p. 55.
- [265] Jonathan Lusthaus. “Trust in the world of cybercrime”. In: *Global Crime* 13.2 (2012), pp. 71–94.
- [266] SingRu Celine Hoe, Murat Kantarcioglu, and Alain Bensoussan. “A game theoretical analysis of lemonizing cybercriminal black markets”. In: *International Conference on Decision and Game Theory for Security*. Springer. 2012, pp. 60–77.
- [267] Jason Franklin et al. “An inquiry into the nature and causes of the wealth of internet miscreants.” In: *ACM conference on Computer and communications security*. 2007, pp. 375–388.
- [268] Chris Edwards. “Ending identity theft and cyber crime”. In: *Biometric Technology Today* 2014.2 (2014), pp. 9–11.
- [269] Roderic Broadhurst. “Developments in the global law enforcement of cyber-crime”. In: *Policing: An International Journal of Police Strategies & Management* 29.3 (2006), pp. 408–433.
- [270] Eva A Vincze. “Challenges in digital forensics”. In: *Police Practice and Research* 17.2 (2016), pp. 183–194.
- [271] BrightPlanet. *Clearing Up Confusion – Deep Web vs. Dark Web*. <https://brightplanet.com/2014/03/clearing-confusion-deep-web-vs-dark-web/>. Accessed: 2017-09-06.
- [272] Flashpoint. *Illuminating the Deep & Dark Web*. 2015. <http://go.flashpoint-intel.com/docs/Illuminating-the-Deep-Dark-Web>. Accessed: 2017-09-06.
- [273] OWL Cybersecurity. *Darknet Series: What is the Darknet?* <https://www.darkowl.com/blog/2017/6/21/darknet-series-what-is-the-darknet>. Accessed: 2017-10-07.
- [274] Andy Greenberg. *Hacker Lexicon: What is the Dark Web?* <https://www.wired.com/2014/11/hacker-lexicon-whats-dark-web/>. Accessed: 2017-09-06.
- [275] npr.org. *Going Dark: The Internet Behind The Internet*. <http://www.npr.org/sections/alltechconsidered/2014/05/25/315821415/going-dark-the-internet-behind-the-internet>. Accessed: 2017-09-06.
- [276] Patrick Howell O’Neill. *How to search the dark net*. <https://www.dailydot.com/debug/how-to-search-the-deep-web/>. Accessed: 2017-09-17.
- [277] Cryptorials. *How To Navigate Your Way Around The Deep Web*. <http://cryptorials.io/how-to-navigate-your-way-around-the-deep-web/>. Accessed: 2017-09-17.
- [278] Paul Bischoff. *Guide: How to access the deep web and darknet*. <https://www.comparitech.com/blog/vpn-privacy/how-to-access-the-deep-web-and-darknet/>. Accessed: 2017-09-17.

- [279] Jenna Kagel. *An Up-To-Date Layman's Guide To Accessing The Deep Web*. <https://www.fastcompany.com/3026989/an-up-to-date-laymans-guide-to-accessing-the-deep-web>. Accessed: 2017-09-17.
- [280] Geoffrey Walters. *How to Access the Dark Web and Deep Web, Safely and Anonymously*. <https://www.addictivetips.com/vpn/access-darknet-deep-web/>. Accessed: 2017-09-18.
- [281] Dan Patterson. *How to safely access and navigate the Dark Web*. <http://www.techrepublic.com/article/how-to-safely-access-and-navigate-the-dark-web/>. Accessed: 2017-09-17.
- [282] DeepDotWeb. *General security precautions when posting online, learn from others' mistakes*. <https://www.deepdotweb.com/jolly-rogers-security-guide-for-beginners/general-security-precautions-when-posting-online-learn-from-others-mistakes/>. Accessed: 2017-09-18.
- [283] The Tor Project. *What is Tor?* <https://www.torproject.org/docs/faq.html.en#WhatIsTor>. Accessed: 2017-09-18.
- [284] The Tor Project. *The Design and Implementation of the Tor Browser*. <https://www.torproject.org/projects/torbrowser/design/>. Accessed: 2017-09-18.
- [285] Tails. *Privacy for anyone anywhere*. <https://tails.boum.org/index.en.html>. Accessed: 2017-09-18.
- [286] Tails. *About*. <https://tails.boum.org/about/index.en.html>. Accessed: 2017-09-18.
- [287] DeepDotWeb. *Staying Safe on the Deep with Tails*. <https://www.deepdotweb.com/2017/01/07/staying-safe-deep-tails/>. Accessed: 2017-09-18.
- [288] Dark Web News. *Dark Web & Deep Web Market List With Up & Down Daily Updated Market Status*. <https://darkwebnews.com/dark-web-market-list/>. Accessed: 2017-10-02.
- [289] Jelena Mirkovic and Peter Reiher. "A taxonomy of DDoS attack and DDoS defense mechanisms". In: *ACM SIGCOMM Computer Communication Review* 34.2 (2004), pp. 39–53.
- [290] DeepDotWeb. *How hidden services DDoSing works?* <https://www.deepdotweb.com/2016/05/06/hidden-services-ddosing-works/>. Accessed: 2017-10-04.
- [291] Uwe Flick. *An Introduction to Qualitative Research*. SAGE Publications, 2014. ISBN: 9781446297728.
- [292] Margaret C Harrell and Melissa A Bradley. "Data collection methods. Semi-structured interviews and focus groups". In: (2009).