Neobanks: Challenges, Risks and Opportunities

Beatrice Corander

Haaga-Helia University of Applied Sciences

Bachelor's Thesis

2021

Bachelor of Business Administration

Abstract

Author(s)
Beatrice Corander

Degree
Bachelor of Business Administration

Report/thesis title
Neobanks: Challenges, Risks and Opportunities

Number of pages and appendix pages
65 + 21

The Neobanks entering the banking industry and market, risks, as well as challenges relating to them have thus far been subject to hardly any academic research. This provides a strong motivation for this thesis.

The purpose of this thesis is to do research on several aspects of Neobanks from both the customer's and society's point of view. The main focus is on the following three facets of Neobanks: (1) challenges, (2) risks, and (3) opportunities, that they have brought with them since their emergence roughly a decade ago. The investigative questions of this thesis are: IQ. 1. What new possibilities have Neobanks brought to banking customers? IQ. 2. What risks are associated with using Neobanks? IQ. 3. Sustainability of the Neobank ecosystem and future challenges on a societal level. These enable answering the research question **"What are the challenges, risks and opportunities linked to Neobanks"**

To better reflect the challenges and risks associated with the rise of Neobanks, are the laws and regulations relating to the general banking industry with an emphasis on anti-money laundering and terrorism financing, as well as the 'Know your customer' (KYC) regulations examined. This thesis additionally investigates the risks related to both Neobanks and the traditional banks that arise particularly from cybercrime associated with technology in the banking industry.

The two largest Neobanks according to European market share were chosen as representatives of the population of Neobanks. Both qualitative and quantitative data were collected, including interviews of financial experts. Through numerical and qualitative summaries of the data the author found that Neobanks may have legally questionable practices related with KYC regulation and that opportunities for money laundering through Neobanks should be taken into serious consideration by authorities and legislative bodies. In conclusion, the future business model, market share and commercial success of Neobanks are difficult to predict, but it can be anticipated that the banking industry will nevertheless face disruptive changes stemming from the widespread adoption of internet technology, rise of cryptocurrencies and the open banking related to EU legislation.

Keywords
Banking Industry, Technology, Neobanks, Traditional Banking, Regulation

Table of contents

1 Introduction

This is a bachelor's thesis for the degree program in International Business (BBA), with a major in Financial Management. Due to the ever-changing banking industry and market, banks that only operate online on an app level, and not in the traditional way with physical branches anymore, have started to enter this market, most intensively during the last six years. This thesis takes a focus on these modern online-only banks (Neobanks) and investigates how they have impacted the banking industry and its customers, positively as well as negatively, and the sustainability of Neobanks' ecosystem. It considers primarily the impact which these Neobanks have had on the clientele from both a potential customer's, as well as the societal and a governmental perspective. Some of the most central questions are accordingly: are these Neobanks trustworthy, should they make a change in their business practices, and what are the risks customers face through the usage of these apps? These are all relevant and important issues that should be considered when new players enter the banking market. They motivate also further research on which type of change might be needed on the legal spectrum, particularly from a customer centric perspective.

1.1 Research Question

This thesis investigates the banking industry, and how the modern online-only banks, Neobanks, have affected the industry, and consequently the traditional banks that existed on the market before Neobanks emerged. The first step in the research is to look at the banking industry, its legislative history, as well as Neobanks, and how they came to be, the short history behind them, and how they've been able to push themselves into the market. After which the differences between the Neobanks and the traditional banks is investigated. Having learned sufficiently about the industry, and the different players on the market, we will dive into the world of technology, and more specifically, consider the impact of technology. Discussion on the Internet of Things (IoT), Open Banking as well as cryptocurrency is also included. When discussing technology, and technology's role in the banking industry, the most relevant target of interest is naturally the banking apps. As a final part of the banking industry technology overview, we will investigate cybercrime and risks associated with technology in the banking industry. Finally, we will provide a brief synopsis of the most important and relevant laws and regulations that apply to the banking industry in Finland, the UK, and the European Union (EU). Now we will formulate the main research question.

Research question:

RQ. What are the challenges, risks and opportunities linked to Neobanks?

Investigative questions:

IQ 1. What new possibilities have Neobanks brought to banking customers?

IQ 2. What risks are associated with using Neobanks?

IQ 3. Sustainability of the Neobank ecosystem and future challenges on a societal level.

1.2 Demarcation

This thesis will focus on traditional banking service providers and modern banking service providers (Neobanks), and how the uprising Neobanks have impacted the banking industry. The traditional banks included in the study will be chosen out of the banks operating in Finland. Two bigger banks, and one smaller bank are chosen according to their market share. The two Neobanks will be chosen according to the highest Neobank market shares in Europe at the time of initiating the data collection for the thesis. This thesis will more specifically take a focus on the b2c market and banking industry sector of the Neobanks in Europe and traditional banks in Finland.

1.3 International Aspect

The international aspect of this thesis comes naturally from the borderless operation of Neobanks, which try to attract customers from an international base. A comparison is made between such banks and traditional banks which may either operate only domestically or in multiple countries with branches, which makes them also international.

1.4 Benefits

The outcome of this thesis will show how and if the Neobanks have changed the b2c sector of the banking industry and market. We will make conclusions about the reasons behind the emergence of Neobanks and try to quantify if they have been able to bring added value to the industry. However, we will also identify the immediate risks associated with operating with the online banking technology. There will be a clear conclusion if the legal sector needs to make a rapid change to ensure safety for customers and the societies in which Neobanks operate.

The benefits of this thesis for the author stem from the new and extensive knowledge the author will obtain about the ever-changing banking industry. Of particular relevance are the risks, laws and regulations, advantages and disadvantages that these changes bring with them to the market. The author can then use this knowledge in a future career in the banking industry.

1.5 Key Concepts

Basic Banking services

‘’Basic banking services include a payment account with basic features and an instrument for using the account (e.g., a debit card and online banking ID), the possibility to withdraw cash, the execution of payment transactions and an electronic means of identification. Basic banking services, on the other hand, do not include accounts with an overdraft facility or various kinds of credit cards.’’ (FIN-FSA 2018.)

Online banking

Internet banking, or also known as web banking, is the notion of conducting financial transactions through the internet. Almost every bank has a form of online banking available for the computer or an app-based service. Meaning the customer can make transactions, deposits, and pay their bills online through these online banking services, instead of the need of a branch. (Frankenfield 2020.)

FinTech

FinTech, short for financial technology. FinTech represents new technology applied to the financial industry. FinTech is used by many sectors, such as the education sector, the banking industry, investment management, as well as cryptocurrency development and usage. (Kagan 2020.)

Neobanks

Banking service providers who provide online-only financial services (Pritchard 2019).

Traditional banking

Traditional banks are banks that provide financial services, have a headquarter, as well as branches all over the country, or operating area (Orlando 2020).

Shell bank

A shell bank is a credit, or financial institution, which does not have a physical presence in any country, and is not part of any conglomerate, in other words, is not regulated by a country's central bank, another bank, or any financial regulator (The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 No. 692).

2 Banking Industry

The banking industry is a very broad term and consequently it can hold a lot of potential topics for discussion and analysis. Within this chapter we will briefly discuss those aspects of the banking industry which are all relevant later on to understand and to answer the research questions of this thesis. We will start by looking into the banking industry in Europe, its history, more specifically the history of banking integration and regulations, and further in particular how the Neobanks came to be. Then we will go more generally into the details of the traditional banking method, what it entails, and how it then differs from the modern banking method, within which Neobanks can be placed, and what different type of services are provided within the banking industry. The thesis discusses further the impact of technology in the banking industry, IoT, open banking, cryptocurrencies in the banking industry, after which we move to banking apps and cybercrime related to the banking industry. Lastly, different laws and regulations relating to the banking industry in Finland, the UK and European Union are reviewed in detail.

2.1 History of European Banking Integration

The main reasoning behind the 1957 Treaty of Rome, was to create a single common market from the highly segmented national market. The single common market was achieved through regulation being recognized as something which can be established and coordinated whenever needed. The European Commission and the Council of Ministers endorsed the “The Abolition of Restrictions on Freedom of Establishment and Freedom to Provide Services for Self-employed Activities of Banks and other Financial Institutions” directive in June of 1973. The national treatment principle is applied in this directive, meaning that the regulation and supervision of all firms operating in one country are treated equally. During this time period there still was no international coordination of the supervision of banks, meaning that banks in different countries could be treated differently with differences in rules. Due to this, there was a need for furthermore harmonizing the regulations, to ease the burden which raised the costs of international operations. (Insead, J 2002.)

In 1977 came the second wave of harmonizing of the banking regulations. This was through the first ever banking directive “The Coordination of Laws, Regulations and Administrative Provisions Relating to the Taking Up and Pursuit of Credit Institutions”, which set down the principles for control in the respective home country. This directive was a good start, but called for further directives, since shortcomings of the first directive were recognized, such as banks having to be authorized by the financial supervisors of a

country if they wished to operate in that specific country, and that most countries required that branches had to be provided with allocated capital, as well as that a foreign bank was supervised by the host country, meaning that their activities were subjected to this country's laws. (Insead, J 2002.)

The White paper published in 1985, called upon a single banking license, and home country control. These principles were incorporated into the Second Banking Directive, Directive 89/646/EEC in 1989. Under this directive have all credit institutions authorized within an EU country the right to open branches or supply cross-border financial services in other EU countries, if they are authorized to provide these in their home country, without being required to get further authorization. In 1994 accepted the Council of Ministers the Deposit Guarantee Scheme Directive 94/19/EC. Under this directive, is a minimum of 20 000 € with a franchise of a maximum 10%, of the consumer depositor's money covered. The EU's vision of creating a widened national market throughout, is created through breaking down the boundaries between countries. This would require a single banking licence across the EU, a home country regulator which would supervise, as well as a single deposit insurer. (Insead, J 2002.)

Neobanks and how they came to be

Due to the 2008 global financial crisis millions of jobs were lost, as well as trillions of dollars of financial capital. Many put the blame mainly on the banking industry, for this loss of financial capital. The lost trust in the traditional banks opened up an opportunity for upstarts to create a new type of financial institution, a Neobank, sometimes known as a challenger bank. Supported by EU's new Payment Services Directive (PSD) integrated into law in November of 2009, was transparency increased in the industry, later being update further by PSD 2, due to which these Neobanks, were able to enter the market. (Ballard 2018.)

A Neobank, online-only bank, internet-only bank, challenger bank or app-based bank, is a banking service provider operating only online, through an app or a webbank, without any physical branches. The banking industry has through history been a monopoly, but due to the progressiveness of EU's financial regulations, an opportunity has been opened up for others to enter the market. Neobanks, not having any physical branches, have been able to save costs, and further offer their basic banking services with lower costs than the traditional players on the market. (Muldrew 2020.) Due to the low, or non-existing costs, are also more people able to afford basic banking services through Neobanks.

Popular Neobanks, like Revolut and N26, have been able to adopt artificial intelligence (AI) and a good user interface design to fuel their chatbots, through which they are able to provide customer support. Neobanks have offered their customers more modern technology products, with their focus on the core part of their business, the apps, when traditional banks have been lagging behind with the technological products and services, they provide their customers. (Muldrew 2020.)

The clear market opportunity for Neobanks has come through the evolution of technology. The younger generation has partially grown up with and adapted their daily life to mobile technology, and this can be clearly seen in the age distribution of the customers of the Neobanks. Revolut and N26, for example, have 40-60% of their customer base in the age range between 25 and 35 years old. Revolut claims to have 42% of their users between 25 and 35 years old. (Muldrew, 2020.) N26 claim to have 25% of their customer's be in the age range of 18-25 years old, and 37% being between 25 and 35 years old, making the total 61% of customer's which are under 35 years old, of their over 1 million customers in France. (N26 2019.)

Figure 1 shows, how many people of the 2 000 study participants aged 18-65, conducted by Censuswide in November of 2018, have a Neobank account (here referred to as challenger bank account). This Figure is clearly supporting the number of customers Revolut and N26 claim to have in the age range 18-35 in total in 2019, as well as showing rapid growth among customers representing younger generations.

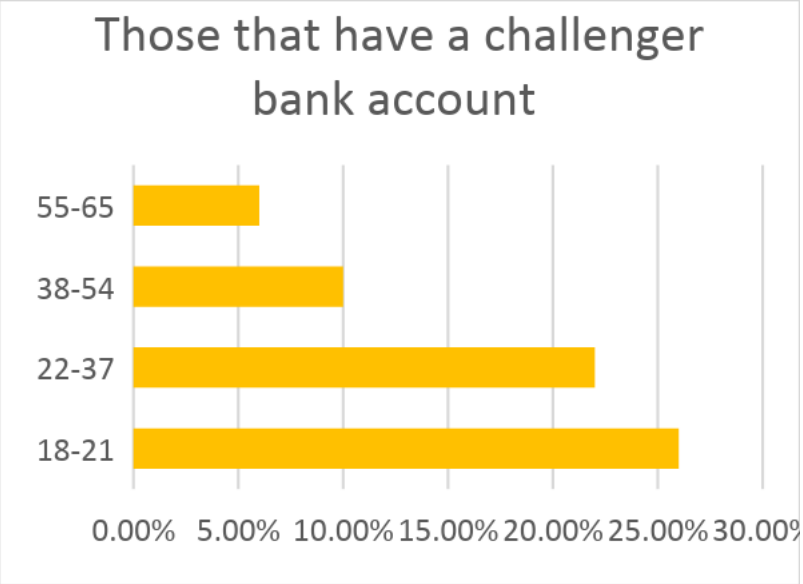


Figure 1. 1 IN 4 MILLENNIALS AND GEN-ZS ARE USING CHALLENGER BANKS WITH MONZO THE MOST POPULAR (Finance Derivative 2021)

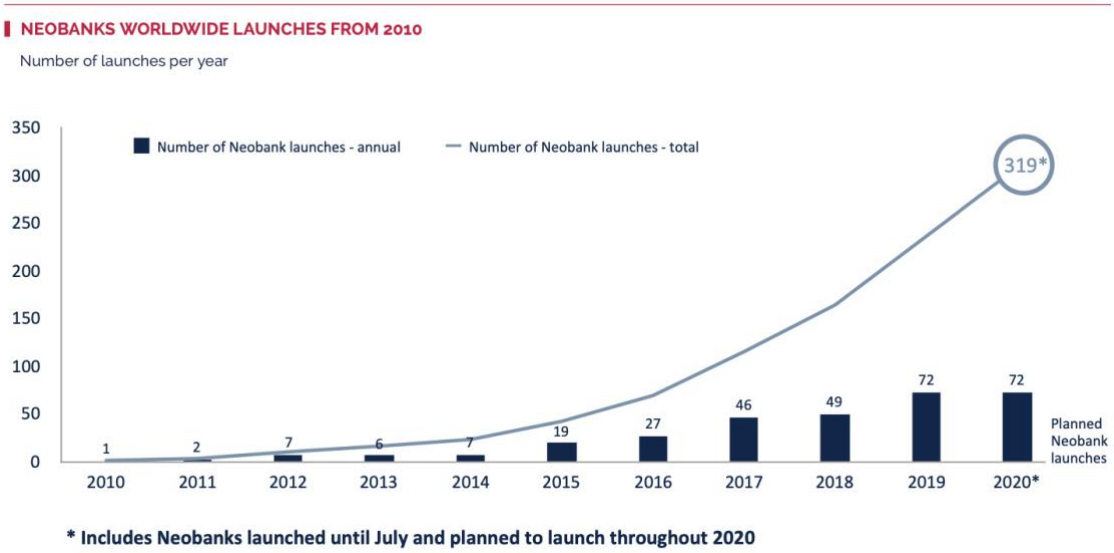


Figure 2. Neobank Worldwide launches from 2010. (exton consulting 2020)

According to Figure 2. above, Neobanks have started to enter the market from 2010, but since 2017, the number of Neobanks has been multiplying rapidly. As shown in Figure 2, there have already been over 300 launched Neobanks in the last 10 years, and when taking a look at Figure 3 below, we see a slow growth for the existing Neobanks on the European market during the 3 first years, and then Revolut experiencing exponential growth, reaching 15 000 000 downloads at the end of 2020.

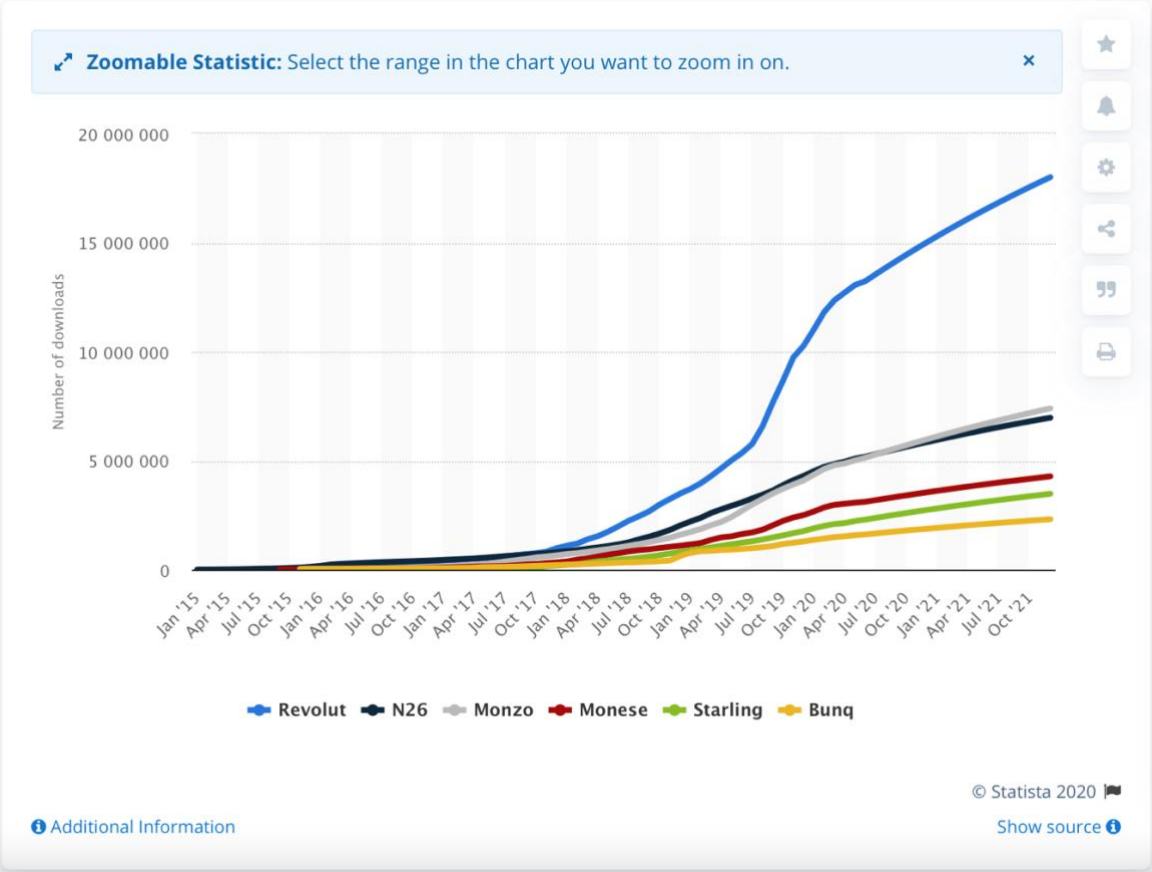


Figure 3. Forecasted number of downloads worldwide of European app-only banks from January 2015 to December 2021, by bank (Statista 2020)

2.2 Traditional Banking and Modern Banking Services

Traditional banking and modern banking differ from each other mostly by the physical factor. Traditional banks have headquarters, as well as branches which a customer can visit and meet a customer service person face to face. This is not the case with modern banking, also referred to as online-only banking. The name online-only bank already gives away the difference, this simply means that these banks operate solely online, and provide their customers customer service and other services, only through online channels, such as e-mail, chat, video call/phone call, or through their own online channels. These banks typically have a smaller product range but attract their customers through “free of fees” slogans and the attractive exchange rates they offer for an internationally mobile customer base. (Orlando 2020.)

Traditional banks have constantly shifted towards a more modern banking model, by realizing the cost benefit of closing some branches and investing in a more online banking operational model. However, according to a survey in 2016 ‘’ which surveyed 55,000 consumers in 32 countries, 60% said they would want to visit a physical branch or speak

with a real person in order to purchase a new financial product or ask for advice.'' (Orlando 2020.)

Banking services that traditional banks provide are usually broader than the services a Neobank would provide. The services a traditional bank would provide, are for example different cards, ranging from Visa cards to MasterCard credit cards, and different types of accounts for different purposes, some for example offering a positive interest rate, depending on the withdrawal restrictions and use purpose. Other examples of services are loans, ranging between housing-loans, student loans, and one-time loans. Further services are saving and investment services, the banks providing the products, such as an investment account, as well as investment services according to the MIFID II standards. Most of the mentioned products and services can be found in Table 1.

The services Neobanks provide are usually the same as some of the services traditional banks provide, but in a more condensed capacity. The services usually include bank accounts, checking and savings, money transferring services, payment services. Neobanks rarely offer any credit, to minimize their risk and to cut down on their costs. (Pritchard 2020.)

Neobanks are not always necessarily banks. They do not have to be registered credit institutions, due to financial services being very regulated as well as the licences being expensive. These non-licenced Neobanks are able to provide services comparable to banking services, by partnering up with licensed banks to then further sell their products and services, as well as by providing transaction services comparable to banking services, via the usage of prepaid debit cards through VISA and Mastercard. (Stevenson, M 2020.) The Neobanks research in this thesis are both licensed banks, meaning they do not fall under this category of non-licensed banks.

2.3 Impact of Technology in the Banking Industry

Technology has had a forceful impact on many industries, and banking is not an exception of this phenomenon. The meaning behind this, has been to facilitate, and then further bring transparency into the industry for the customers.

According to the Forbes article written by Shevlin (2020) on the five hottest technologies in banking for 2020, number one was digital account opening, and challenging the traditional banks on the question why it is made so difficult. According to Shevlin (2020) the answer to this question lies in the regulatory and compliance approach banks have

been taking to this. But Shevlin argues that the banks should focus first and foremost on redesigning their process, and later work on the risk reduction and regulatory aspect. This can of course be argued to the contrary, meaning that the fact that banks have the risk and regulatory point of view as the first step, does make the customers feel safer.

The increasing number of people using mobile devices to conduct their banking affairs has been seen in Europe as well as USA and Australia according to the ING International survey of Mobile Banking 2018. This is a very expected change, since the access to a smart phone and internet has increased rapidly during the last years. According to the ING International survey 58% of people are continuing with their main bank service provider, or a so-called traditional banking service due to the monetary services offered, but the rest are choosing to take part of the new age of banking services, changing their banking service provider to a more modern finance technology, which typically corresponds to the Neobanks. According to the same study, the fraction of European smartphone owners who used their smartphone to conduct any type of banking, went up from 48% in 2017, to 61% in 2018. This illustrates the rapid change happening within the banking industry, when combining technology, smart phones, and online banking services together.

As seen from Figure 4 below traditional banks still play a key role in European consumers' banking life. As mentioned earlier, 58% of people in Europe, have only used their main (traditional) bank, to conduct their daily banking. The rest, almost 40%, have ventured outside their traditional banking services provider, to some other financial service provider. According to the study conducted, 16% of the population are of the opinion, that they would get more value from elsewhere than their main, traditional banking service provider, by paying less for the services. Figure 5 shows that 21% of the surveyed population use some other financial service provider than their main banking service provider to make money transfers, and 13% some other digital banking service. This study shows how these digital service providers are rapidly becoming more popular around the world, but especially in Europe (See Figure 5).

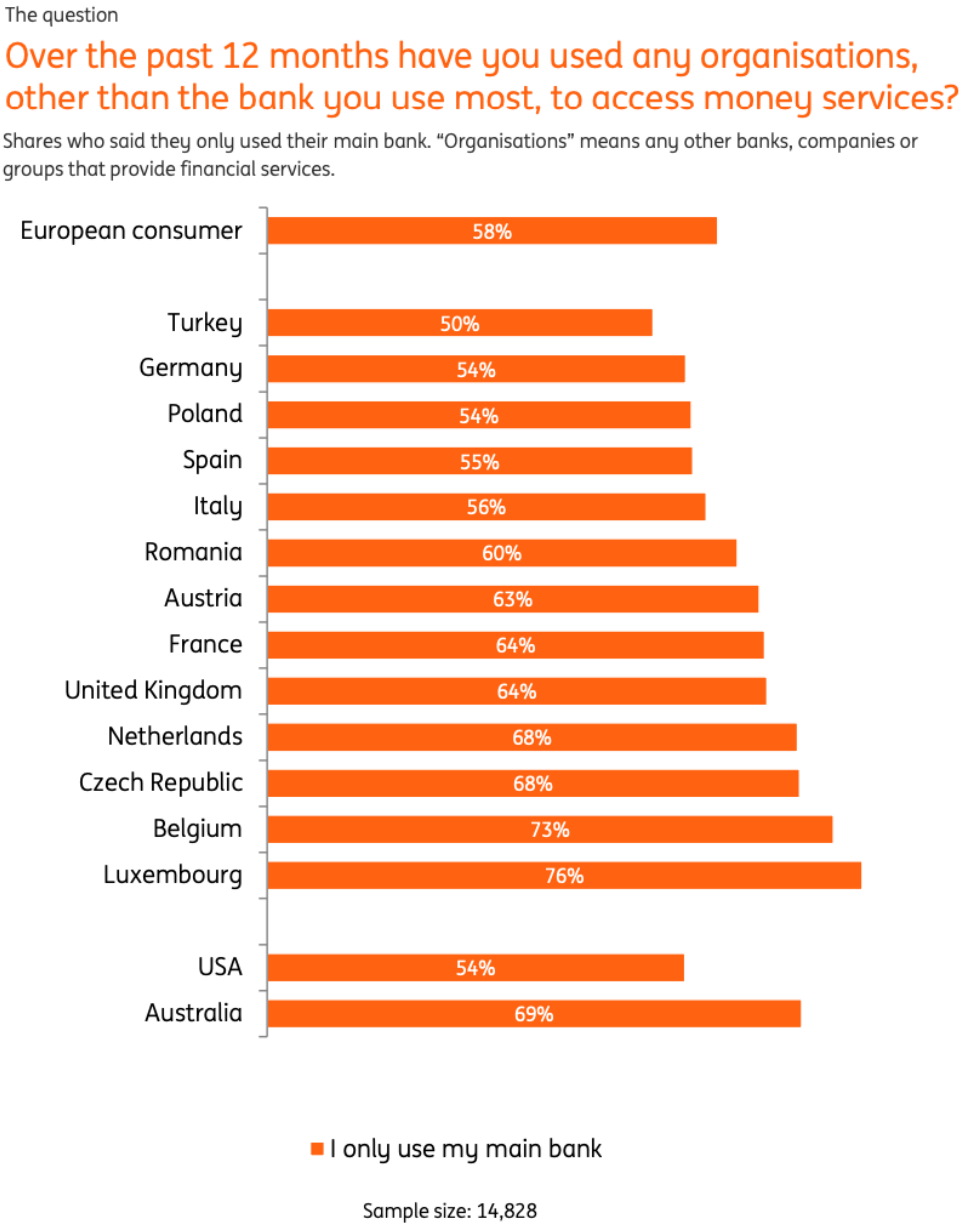


Figure 4. General summary of answers per country to the use of financial organisations to access money services. (ING 2018.)

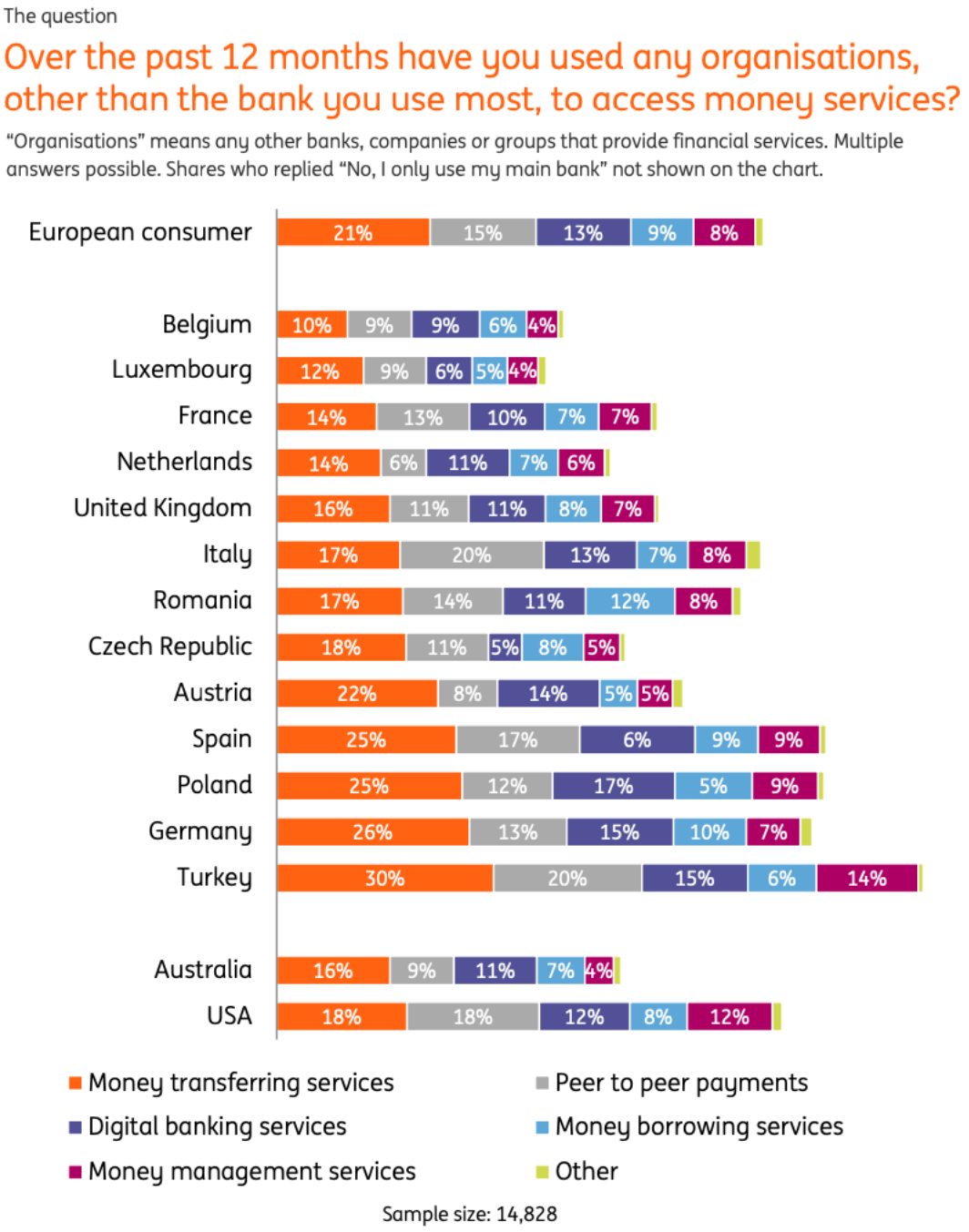


Figure 5. Detailed summary of answers per country to the use of financial organisations to access money services (ING 2018.)

Internet of things

Internet of things, (IoT), has become a growing topic of conversation both in the business, as well as people's private lives. IoT has the potential to change the way people work and live. It is the concept of any device being connected with an on and off switch to the internet or to each other. To this category belong consumer devices such as coffee

makers, washing machines, headphones, wearable devices, and cell phones, but naturally also a very broad spectrum of devices in a multitude of industries. According to Gartner there were going to be 26 billion connected devices by the end of 2020, and others estimate this number to be even higher. Internet of things is a large, connected network of different devices as well as people, and these connections go between people and people, people and things, and things and things. (Morgan J, 2014.)

Open banking

Open banking in Europe has become familiar, due to the implementation in September of 2019 of the Second Payment Services Directive, the PSD 2 act. This act supports innovation and creativity in the payments field, which leads to more choices and a better control over the consumers own financial data and information. The PSD 2 act also supports open interfaces, so that the consumers are able to make payments online through a third-party interface, due to the banks being required to share their interfaces with these third parties, naturally with the consent of the consumer. This is not solely meant as a payment method for e-commerce, but also for credit institutions as well as other financial services providers. (Trustly 2021.)

Cryptocurrency and Cryptocurrency in Banking

Cryptocurrency, also known as cryptos, is a medium of exchange, it is an equivalent to money since the buyer and seller both have the knowledge of the value. Cryptocurrency is being stored as well as created 100% electronically in the blockchain, through encryption. This encryption has the control over the creation of the monetary units, as well as the transfer of the funds. The most well-known example of a cryptocurrency is Bitcoin. (PWC 2021.)

There is no inherent value for cryptocurrency, since it cannot be cashed into other assets, which can be done for example with gold. The network of the cryptocurrency is totally decentralized, as it is not supplied through any central bank. (PWC 2021.)

Cryptocurrency in banking is on the rise, and the banking industry should start adopting cryptocurrencies according to the Boston Consulting Group. However, there is a good reason to be cautious of the value which it has as an asset class. The cryptocurrencies have experienced volatility throughout the COVID-19 crisis, and the reputation of them as

a currency has been damaged through association with criminal activities, such as the hacking of Twitter in July of 2020. (Abedine & al. 2020.)

The European Union has been working on towards the tightening of regulations regarding cryptocurrencies already in 2018. Although it has not been very clear yet how this will affect the business practices around the field. This directive will be discussed further in chapter 2.4 Banking and Financial Service Laws and Regulations, subsection; Eu banking laws and regulations, sub-subsection; Fifth Anti-Money Laundering Directive (5AMLD).

2.3.1 Banking Apps

Most banks today provide a banking application, better known as banking apps. A bank without a banking app would not be able to compete with the other actors on the market. A majority of consumers would rate such a bank negatively, and most likely switch to another bank, if the bank would not provide online banking services with the same standards as the other banks on the market.

Access to the customers' accounts, products and services has been made considerably easier and more transparent through banking apps. The apps make managing your personal daily banking much easier, since a customer can transfer money between own accounts or make a payment to someone else's account with the press of a few buttons. You can also quickly block your card in case of it getting stolen, edit your daily usage restrictions, and in most banking apps, even access you bank cards pin code in case you happened to forget it. The apps have even made investing much easier and quicker, because when you can manage your investment just through your phone, you can make quick investment decisions when needed.

2.3.2 Cybercrime and Risks Associated with Technology in the Banking Industry

Cybercrime has been on a constant rise, since the beginning of a wide-spread use of internet technology and it has become the biggest risk factor associated with technology within the banking industry. Based on a study conducted by Accenture (2019) with companies from 11 different countries around the world, and 15 different industries, it was estimated that the average revenue opportunity risk, meaning the possible loss of revenue due to cybercrime, in the banking industry, and the capital market, will be $394 billion between 2019 and 2023. These numbers are very alarming for the banking industry, since

the same study also shows that the banking industry, has been leading this risk category for the last few years.

As shown in Figure 6 below, the annual cost of cybercrime across all 15 surveyed fields, was biggest for malware, and in second place were web-based attacks. These two biggest types of cybercrime attacks correspond to slightly over $4,8 million as an average annual cost for each company taking part in the study, over a third of the total average annual cost in 2018 $13,0 million. Other types of cybercrimes are malicious insider and code attacks, phishing and social engineering attacks, ransomware, as well as botnets. Also, according to Accenture's study, ransomware attacks have grown most, 21% from 2017 to 2018, and second in growth were malicious insider attacks, with a 15% growth.

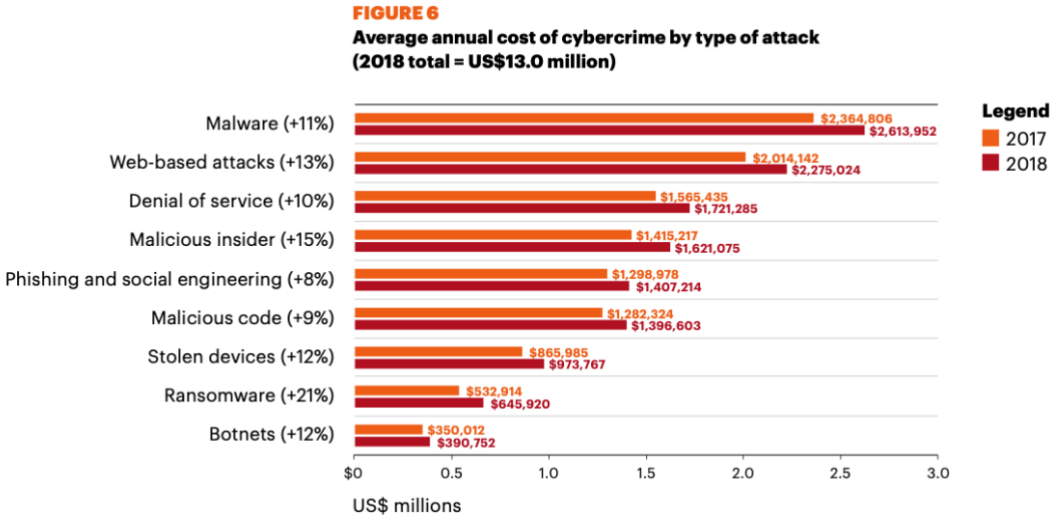


Figure 6. Average annual cost of cybercrime by type of attack (Accenture 2019.)

Other risks associated with technology than cybercrime, in the banking industry, are having an ineffective IT strategy, old and outdated technology used by the financial institutions, as well as mergers and acquisition (HCL, 2021). Companies in the financial sector are more likely to be a target for cybercriminals than companies in other industries, the average annual cost of cybercrime for the banking industry in 2017 was 16,55 million US dollars and then rose to 18,37 million US dollars in 2018 (Accenture 2019).

2.4 Banking and Financial Service Laws and Regulations

In this subchapter the banking laws and regulations relevant for the thesis RQ and IQs are reviewed. The laws and regulations are presented in an order of proceeding from the more general to more specific topics. All the topics are nevertheless considered to be equally important for understanding the underlying legal framework concerning Neobanks

and the traditional banks. The European Union has regulated the banking industry through EU banking and financial service laws and regulations. Companies providing their services and/or operating in EU countries, have to follow these laws. After considering EU banking laws and regulation we will go through some regulations relating to banking in the UK, and lastly go through Finnish banking laws and regulations. The main regulations discussed throughout EU, UK and Finnish regulations are Anti-Money Laundering AML, and Know Your Customer (KYC).

EU banking laws and Regulations

The Directives, Acts, Regulations and Policies are put in place, and enforced by the European union and the European Banking Authority (EBA). In the following sub-subchapters, the author writes about some key important Directives in the EU as well as other regulatory frameworks. The topics discussed are Anti-Money Laundering (AML), Know Your Customer (KYC), as well as Payment Services (PSD 1 & 2).

DIRECTIVE 2014/92/EU on the comparability of fees related to payment accounts, payment account switching and access to payment accounts with basic features

In section 4 of the directive, it discusses the instruction and guide on the right to a bank account. As indicated in the resolution of 4th of July 2012, the European Parliament indicated the need for improvement and development of retail banking's internal market, with some recommendations to the Commission on Access to Basic Banking Services. There is a barrier created between the deployment of a fully integrated market which would then contribute to lower competition within the retail banking sector, due to lack of transparency, comparability of fees, as well as the difficulties in switching payment accounts. There is a high priority on tackling these issues in the market. (DIRECTIVE 2014/92/EU.)

The internal market at the moment needs a higher quality standard, to stop the challenges for payment service provider when entering a new market and exercising their rights to establish and provide payment services. This is then discussed in section 5 of the directive and further elaborated on in section 6. Section 7 discusses that the potential in the European Union is not fully used projecting the existing demand of payment account services with potential consumers which for different reasons do not open account e.g., if they get denied the account, or if the service providers' product selection is not wide and sufficient enough. New service providers would be motivated to enter the market if there

would be a broader consumer engagement within the internal market. (DIRECTIVE 2014/92/EU.)

A self-regulatory initiative (which was proposed by the banking industry) on a European Union level for comparability and transparency of fees were considered, but never realized due to a lack of a final agreement. This was discussed in section 8 of the Directive. Section 9 mentions, that the long term smooth and effective financial mobility would be supported through systematically set rules, which would combat the problem with the low customer mobility and better, the tendering of service providers and their comparability between services and fees of payment accounts, as well as encourage the switching of payment accounts. This would also combat the discrimination of consumers due to their residential status and or their intention of using the account in a cross-border manner. The content of this Directive, should be applied to all payment service providers regarding the comparability of fees and switching of payment accounts, according to the Directive 2007/64/EC. (DIRECTIVE 2014/92/EU.)

Fifth Anti-Money Laundering Directive (5AMLD)

EU took steps to open up the cryptocurrency market in the EU in the fifth Anti-Money laundering Directive. The directive has made important changes to virtual currency as well as the beneficial ownership of companies and trusts. The fifth directive (5AMLD) was published in 2016 whiles countries were still making changes according to the earlier directive (4AMLD). The 5AMLD was an update based on the 4AMLD and was done with such a narrow timeline due to the need of further change and strengthening of the Anti-Money Laundering and Combating of Financing of Terrorism (AML/CFT) Law in the EU. The changes made to the 4AMLD, and the most important categories are:

1. the regulation of virtual currency,
2. information on beneficial owners,
3. the use of prepaid card,
4. powers of financial intelligence units and supervisors, and;
5. due diligence for high-risk countries. Relating to this, have the EU law makers made a proposal for a directive on countering money laundering by criminal law. (Linklaters 2021.)

The section in the 5AMLD on virtual currency, broadens the AML/CFT regulatory perimeters control. It also brings providers of exchange services between virtual currencies, and fiat currencies (government-issued currency not backed by a commodity such as gold), which are the platforms exchanging money to cryptocurrency as well as the providers of custodian wallets (a digital wallet, which keeps the private keys of the customer as well as backs up the assets and providers security), into the scope. These

service providers are both included into the 4AMLD's obliged entity definition, as well as new definitions are established for both service providers, the virtual currency and the custodian wallet. Before this change, hasn't a service provider been required to identify suspicious activity, which they are now required to do under the 5AMLD. This extension of the regulation perimeter has been designed, to prevent organized crime from being able to use virtual currency, to exploit the anonymity of the virtual currency transactions, as well as to improve the monitoring of the users, but not slowing or stopping the progress and development. (Linklaters 2021.)

The study requested by the TAX3 committee on Cryptocurrencies and blockchain, also specifically asks the question and discusses, if some aspects of cryptocurrencies should be criminally sanctioned and banned. The study asked why is, the degree of anonymity some provide, truly necessary, and if the level of anonymity attends too much to criminal activity. The council's conclusion on how to respond to malicious cyber activities, in April of 2018, seems to be in line with the suggestion of imposing a ban and criminally sanctioning the aspects of it not being possible to verify the users. (Houben & Snyers 2018.)

EBA Report on Competent Authorities' Approaches to the Anti-Money Laundering and Countering the Financing of Terrorism Supervision of Banks

The findings of the first year of ongoing reviews conducted by the European Banking Industry (EBA) and their supporting team of AML/CFT experts, are summaries in the report on competent authorities' approaches to the anti-money laundering and countering the financing of terrorism supervision of banks. The report also describes how the competent authorities in this year's sample apply the risk-based approach set out in international standards. In the findings it was stated that the incorporation of the international and national risks in their assessments was found to be difficult, but the authorities were still aware of the need of addressing these risks. All of the authorities had taken steps to assess the risks associated with money laundering and terrorism financing, but there were challenges relating to the number of risk factors used in the determining of a risk rating, meaning that the rating was not always appropriate, related to the risk assessments of individual banks. The competent authorities are required, by the supervision guidelines, to assess risks related to money laundering and terrorism financing, associated with individual institutions. Some of the competent authorities had put in place, a supervision strategy for the banking sector relating to AML/CFT but did not always reflect the outcomes of the competent authority's money laundering and terrorism

financing risk assessments. There were supervisory authorities, which did not have a strategy set in place for the risk assessment of AML/CFT, leading to some Member States' banks not having ever been supervised for the purpose of AML/CFT. Due to the findings of this report, the competent authorities have been recommended to implement an overall supervisory strategy, to set clear objectives, and to ensure that even the medium and low risk ranked banks on the AML/CFT perspective are being included in their supervisory strategy as well as their inspection plan. The review team also recommended for the competent authorities, to implement an international supervisory cooperation strategy, to be able to see as broad of a risk scale relating to money laundering and terrorism financing. The authorities should work closely with other competent authorities and stakeholders on a domestic scale, to ensure AML/CFT supervision on the territory of banks. (European Banking Authority 2020.)

Payment services (PSD 1) – Directive 2007/64/EC

The PSD 1 directive sets down the rules for the payment services, such as credit transfers, direct debit payments as well as direct card payments. Obligations linked to the usage of payment services, as well as information requirements linked to payment service providers are included in these rules. This directives' purpose, is to state guidelines for the execution of payment transactions related to electronic money, defined in article 1(3)(b) of Directive 2000/46/EC. The purpose of this directive is though not to regulate the issuance of electronic money, nor to change the prudential regulation of electronic money institutions according to the 2000/46/EC directive. Due to this, payment institutions shouldn't be allowed to issue electronic money. (Directive 2007.)

It is crucial to establish a single license for all payment service providers, not connected to taking deposits or issuing electronic money, to remove legal barriers of market entry. As a result of this, is the introduction of a new category of payment service providers called payment institutions is appropriate.

Payment services (PSD 2) – Directive

The previous PSD act was adapted in 2007. This act created the foundation for the Single Euro Payments Area (SEPA), as well as a single market for payments. The digitalization of the European economy has steadily progressed since the implementation of PSD. Emerging new players on the market providing online payment services has provided a need for an update to the PSD act, and consequently the act was updated, leading to the

new PSD 2 act. The purposes behind this update were: to make payments safer, consumer protection, adapt innovation, as well as create an even playing field for all the players on the market including new ones. (European Payments Council 2017.)

The most important changes to the PSD act implemented in the PSD 2 act, are the acknowledgement of new players accessing the customers' payment accounts, an increased security of internet payments using strong customer authentication (SCA), and a broader geographical reach. The acknowledgement of new players accessing the customers' payment account, is done through new players being registered, licensed, and then regulated at the EU level. The barriers are removed between these companies, making the market more transparent, and increasing competition. This is then supposed to translate into lower costs for the customers. (European Payments Council 2017.)

These new players on the market will be able to, with the consent of the customer, access the customers' payment account. Through this, will the holding institution of the payment account, provide access to the account, to these new players through e.g., an Application Programming Interface (API). The increased security of internet payments, through Strong Customer Authentication (SCA), has the purpose to reduce the risk of fraud of electronic payment transactions, as well as to enhance the protection of customer data. This increased security is done through SCA, which means that two or more factors are used, of the following: something only the user knows, a password or a PIN-code etc., something only the user possesses such as a physical card, or something that is part of the user, such as a fingerprint, or a voice recognition. (European Payments Council 2017.)

United Kingdom Banking Regulation

The Prudential Regulation Authority (PRA) regulates the UK banking sector for prudential purposes. This authority is part of the Bank of England, therefor the UK central bank as well. The Financial Conduct Authority (FCA), which has the responsibility to regulate the banking sector, works closely with the PRA. The PRA published a paper in March of 2016, on their approach on the banking supervision, with the approach to authorising and supervising international banks in the light of Brexit. The FCA's main operational objectives, to ensure that the financial market functions well, is to secure an appropriate degree of protection for the consumers, is to protect and enhance the integrity of the UK's financial system, as well as to promote effective competition with the interest of the consumer in the regulated financial service market. The most common issues within enforcement, have been during the previous years in failing to collaborate with the

appropriate regulatory authorities, control failures with anti-money laundering, failing to assess, report and maintain financial resources. The regulatory authorities enforce banking laws and regulations, with sanctions, such as withdrawal of authorisation, fines, banning orders as well as public disclosure of non-compliance, meaning they would lose face in the eyes of the consumers. (Slaughter and May 2019.)

Bank of England and Financial Services Act 2016

In the Bank of England and Financial Services Act update in 2016, section 30 considers money laundering, and the changes made to this act in regard to Money Laundering. The FCA must issue guidance to regulated entities on the definition of one or more categories of politically exposed persons (PEP), prior to relevant regulations coming into force. The act also mentions, that for the purpose of the earlier mentioned relevant regulation regarding PEP, means the regulatory transposing into UK law, measures which the EU Member States must implement for the purpose of combating money laundering, which contains references to PEPs. (Bank of England and Financial Services Act 2016.)

Anti-money laundering registration

A business run in the financial sector, may need to register themselves with an anti-money laundering scheme, meaning they will have to follow anti-money laundering regulations. Businesses in the financial and credit sector, need to follow the regulations. (GOV.UK 2021.)

UK Money Laundering Regulations

The UK laws and guidance's on anti-money laundering and terrorism financing are set in the Proceeds of Crime Act (POCA) 2002. This Act is based upon the Serious Organised Crime and Police Act (SOCPA) 2005, the Money Laundering, Terrorism Financing and Transfer of Funds Regulations 2017, as well as on the Terrorism Act 2000. The aim of the Money Laundering Regulation on money laundering, terrorism financing and transference of funds put in effect on 26th of June 2017 is to ensure the UK's anti-money laundering regime, implements the Fourth Money Laundering Directive of the EU, and that it follows the Financial Action Task Force's recommendations and standards. (IFA 2021.)

In 2019 was the Money Laundering and Terrorism Financing Regulations 2017 updated and amended. These amendments came into effect on 10th of January 2020 and were

implemented in accordance with the Fifth Money Laundering Directive of the EU and contains changes to the due diligence related to the new requirements of reporting information on discrepancies between the information collected during customer due diligence and the information on the persons with significant control register, to the registrar of companies; Companies House. (IFA 2021.)

Financial Services – The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 No. 692 – (United Kingdom)

This bill of regulations identifies the relevant persons to whom the regulations should apply, then imposes the requirements for risk assessment to identify the money laundering and terrorism financing risks (The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 No. 692 p.116-117). Companies are required to identify and monitor their clients and their use of the services provided. According to the money laundering, terrorist financing and transfer of funds regulations are the companies in the regulated sector required to write a risk assessment, which will assist the company in the development of policies, procedures as well as controls, risks related money laundering and terrorism financing. The assessment will be able to detect and prevent money laundering and terrorism financing. (The Law Society 2020.)

In the section on customer due diligence, is the identification and verification of the customers, based on a reliable source such as a passport, regulated. (The Law Society 2020.) According to the enhanced customer due diligence, are the credit and financial institutions required to collect information on the correspondent, meaning the credit or financial institution the domestic credit or financial institution has a contract with. This corresponding institution is required to obtain sufficient information, verify, identify the customers according to customer due diligence on the correspondents' customers. A credit and financial institution is not allowed to have a correspondence relationship with a shell bank, nor to continue a corresponding relationship with a shell bank. (The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 No. 692.)

Enhanced due diligence (EDD) must be applied, regarding any transaction or business relationship involving person or persons which are established in a high risk third country. It must also be applied when the transaction or the business relationship is involving a politically exposed person (PEP), including a person related to a PEP person. The EDD

must also be applied in any situation which present a high risk of money laundering and terrorism financing. (The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 No. 692.)

Know Your Customer (KYC) – (United Kingdom)

Know your customer (KYC), is the process meant for the verification and identification of your customers, clients and suppliers. Knowing your customer, is all about doing your due diligence, by researching company data, checking sanction lists, lists on politically exposed persons, as well as watchlists. It is extremely important for organisations to have sufficient due-diligence processes in place, to ensure that they are act accordingly and by the most up to date domestic as well as international KYC standards. A very important part of the KYC due-diligence is the monitoring of sanction- and watchlists, since illegal activities can result in having sanctions set against an organisation or individual person. These activities might include money laundering, the financing of terrorism, acts of terrorism, drug trafficking, human-rights violations, arms distribution, or violation of international treaties. (LexisNexis 2021.)

Finnish Banking Laws and Regulations

Banks operating in Finland have to not only follow the laws put in place by the European Union, but also Finland's own laws regarding banking. Laws within relation to credit institutions. Finanssivalvonta, the Financial Supervisory Authority (FIN-FSA), being the institution overseeing that all credit institutions in Finland follow the laws within relation to credit institutions. Within this category falls banks operating in Finland as well. (FIN-FSA 2018a.)

FIN-FSA oversees that all deposit banks, as well as credit institutions follow all laws, as well as the regulations and requirements put in place by FIN-FSA, which are concerning the deposit banks and credit institutions solvency, risk management, as well as risk taking (FIN-FSA 2018a).

According to FIN-FSA, the main acts on the banking financial market, are the act on preventing money laundering and terrorism financing (AML), consumer protection act, the limited liability companies act, auditing act as well as the accounting act. Credit institutions, payment service providers and mortgage credit intermediaries, are under the banking sector main regulations. Under the payment service providers regulations can be

found the PSD 2 act, maksupalvelulaki (law on payment services) (290/2010), maksulaitoslaki (the law on payment institutions) (297/2017), laki rahanpesun ja terrorismin rahoittamisen estämisestä (the law of the prevention of money laundering and the financing of terrorism) (444/2017), Valtiovarainministeriön asetus maksulaitoksen toimilupahakemukseen liitettävistä selvityksistä (the regulation on the attachments needed for the payment institution's license application, by the Ministry of Finance) (1040/2017), and Valtiovarainministeriön asetus maksulaitoksen omien varojen laskemisessa käytettävistä menetelmistä (the regulation on the methods used in the calculation of the payment institution's own funds, by the Ministry of Finance) (1039/2017). (FIN-FSA, 2018b.)

Laki Talletuspankkien toiminnasta (Law on the activities of deposit banks) 1268/1990

The law on the activities of deposit banks, which in addition is also applied to the provisions of the Commercial Banking Act (1269/90), the Savings Banking Act (1270/90), the Cooperative Banking Act (1271/90) or the Act on Postipankki Oy (972/87) (Laki talletuspankkien toiminnasta 1268/1990).

According to section 2§, only a deposit bank is allowed to take deposits from the public, but the right of the Bank of Finland as well as cooperative engaged in savings bank operations are regulated separately (Laki talletuspankkien toiminnasta 1268/1990).

According to section 6§ only a deposit bank is allowed to us the word "pankki" (bank) in the name of the business. Also, the name of the business of a deposit bank must include the word "pankki" (bank), as well as indicate the company form of the bank. In addition to the deposit banks, only the Bank of Finland, the Nordic Investment Bank, and the Mortgage Bank is allowed to use the name "pankki" (bank) in their business name, or to describe their business activities. The term is allowed to be used in the name of the business, or to describe the business activity, only if it is clear that the term does not mislead in regard to the business practices. (Laki talletuspankkien toiminnasta 1268/1990.)

The penalty according to section 60§ for acting against sections 2§ taking deposits from the public or section 6§, using the "pankki" (bank) in their business name, shall be fined or imprisoned for a maximum of six months, unless the act has been mild or if a more severe

punishment is provided elsewhere in the law (Laki talletuspankkien toiminnasta 1268/1990).

In section 10§ of the law, it is stated that when funds are deposited to the bank an agreement of the deposit must be concluded between the account opener and the bank. The account opener must always be identified and on this said agreement, there must be sufficient information about the account opener, owner as well as the allowed users of the account. (Laki talletuspankkien toiminnasta 1268/1990.)

Laki rahanpesun selvittelykeskuksesta (The law regulating the money laundering financial intelligence unit) 28.6.2017/445

The application scope of this law is the regulation of the money laundering financial intelligence unit, the prevention of money laundering, the prevention of the financing of terrorism, the detection as well as the investigation register (Laki rahanpesun selvittelykeskuksesta 28.6.2017/445).

Section 3 § goes through the prevention of money laundering and the prevention of the financing of terrorism, the detection as well as the investigation register. The money laundering financial intelligence unit has a money laundering register, which they are the administrator of. The register is meant for the money laundering financial intelligence unit, as a permanent personal data register upheld through automated data processing for the prevention of the financing of terrorism, the detection as well as the investigation. The register may contain the information as well as the documents received for the purpose of the tasks provided in section 2§ (money laundering financial intelligence unit and its tasks) as well as the necessary information and documents received under section 4§ (the right of the money laundering financial intelligence unit to receive and disclose information) and 5§ (the exchange of information). In the register it is allowed to save the names and employer information of the person who has made the notification, as well as the following information of the person to whom the notification relates; the names; the date, country and state of birth; the personal identity number; the information on the document used for identification; the gender; the mother tongue; the citizenship, statelessness or nationality of the person; the home state; the marital status; the profession; the address, telephone number and other contact information; information on the death or declaration of death of the person; the customer number issued by the authorities; the business ID number. It also is allowed to save; the bank and payment account information as well as safe deposit box information, and the customer ship and the customer account information; the names

and addresses of the parents of the alien information in the travel document and other necessary information related to the entry of the country as well as the border crossing; and a photograph, if storage is necessary for the handling of the matter. (Laki rahanpesun selvittelykeskuksesta 28.6.2017/445.)

Laki rahanpesun ja terrorismin rahoittamisen estämisestä (the law of the prevention of money laundering and the financing of terrorism) 28.6.2017/444

In section 1 § of the first chapter of this law is the purpose of the law stated, which is to prevent money laundering and the financing of terrorism, to promote detection and investigation of activities related to the earlier mentioned once, and to enhance the recovery and tracing of proceeds related to crime (Laki rahanpesun ja terrorismin rahoittamisen estämisestä 28.6.2017/444).

In chapter 3 the law discussed the knowing of your customers, further abbreviated as KYC. In section 1 § of this chapter it is stated that if the notifiable party is not able to execute the KYC process as it has been established, is the notifiable party not allowed to start a customer relationship, perform a transaction, or maintain a business relationship. If the notifiable is a credit institution, is the institution not allowed to perform a payment transaction through a payment account if they aren't able to complete the KYC process. The notifiable is also required to access the need to report on the suspicious business practices. The notifier shall not continue further with the KYC process, if they deem it to jeopardize the reporting of the suspicious business practices. When assessing the money laundering and the financing of terrorism risks related to the customer relationship on new, and already existing customers, is the assessor required to consider the risks related to countries or the geographical areas, products, services and transactions, and the distribution channels as well as the technologies (risk-based assessment). (1.6.2018/406). (Laki rahanpesun ja terrorismin rahoittamisen estämisestä 28.6.2017/444.)

The measures set out in chapter 2 section 1§ of this law, shall be followed throughout the whole customer relationship, as well as always be based on the risk-based assessment. The notifier is also required to comply with the acts' regarding the KYC process, when the notifier has a statutory obligation to contact the customer during the calendar year, to verify relevant information regarding the beneficial owner or when the notifier has such an obligation under the law on the national implementation and application of the provisions of the council directive on administrative cooperation in the field of taxation and the repeal

of the directive 77/799/EEC. (26.4.2019/573). (Laki rahanpesun ja terrorismin rahoittamisen estämisestä 28.6.2017/444.)

The notifier is required to be able to demonstrate that they have used methods to identify customers and continuous monitory processes provided for in this law regarding risks relating to money laundering and the financing of terrorism, to the supervisory authority or a person appointed to the position of supervisor (Laki rahanpesun ja terrorismin rahoittamisen estämisestä 28.6.2017/444).

In section 2§ of chapter 3 of this law, is the identification of a customer discussed, as well as the authentication of a customer. The notifier is required to identify the customers identity, when establishing a regular customer relationship, as well as in the situations listed as following:

1. When the total amount of the transaction or interconnected transactions are summed up to be at least 10 000 EUR and the customer relationship is occasional, or in the case of a transfer being more then 1 000 EUR and it is related to the Payer Information Regulation article 3 section 9§.
2. The amount of the transaction or interconnected transactions in cash are summed to be at least 10 000 EUR, and the customer relationship is occasional.
3. If the transaction is suspicious, or the notifier suspects the transaction to include funds to be used for the financing of terrorism or an attempt punishable by it.
4. If the notifier suspects the reliability or sufficiency of the identification and authentication information relating to the customer. (Laki rahanpesun ja terrorismin rahoittamisen estämisestä 28.6.2017/444.)

In section 3§ of chapter 3 is the customer information and its storage discussed. The notifier is required to keep all of the information related to the knowing of your customer and their transactions up to date and relevant. The information needs to be stored in a reliable manner for the period of five years, after the ending of a regular customer relationship. In case of an occasional transaction, is the information regarding the transaction required to be stored for five years from the date of the transaction. (1.6.2018/406). (Laki rahanpesun ja terrorismin rahoittamisen estämisestä 28.6.2017/444.)

The following information regarding KYC is required to be stored: the name, date of birth, personal identity number and address; the name, date of birth and personal identity number of the beneficiary; the full name, registration number, registration date and registration authority of the legal person, and if necessary, the articles of association; the full names, dates of birth and nationalities of the members of the board of directors or similar decision-making body of the legal person; the field of the activity of the legal person. Information also required to be stored, is the name, date of birth and Finnish

personal identity number of the beneficial owners and, in the absence thereof, citizenship and, also if necessary, a more detailed description of the ownership and control structure or, if the beneficial owner has not been identified, the information referred to in Chapter 1, Section 5§, Subsection 4 of this law. The information of the name of the document used for identification, the document number or other identifying information and the issuer or a copy of the document or, if the customer is remotely identified, information on the procedure or sources used for verification, is also required to be stored. The information on the customer's activities, the quality and scope of business, financial position, the reasons for the use of the transaction or service and information on the origin of funds and other information referred to in section 4§ subsection 1, acquired to know the customer, of this law. The information necessary for the fulfilment of the reporting obligation provided for in section 4§ subsection 3, and the enhanced duty of knowledge related to a politically influential person (PEP) provided for in section 13§. The number of the bank or payment account, the name of the account holder or right holder and the date of opening and closing of the account, as well as other identifying information related to the account, so far as they are not included in items 1–9 and the retention is appropriate given the nature of the reporting business; legal obstacle, is also required to be stored. The name of the lessee of the safe deposit box and other identifying information related to the rent of the safe deposit box, as long as they are not included in items 1–9 and the length of the lease period and retention is appropriate given the nature of the notifiable business and is not prevented by other legislation, also need to be store. The methods of electronic identification provided for in Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services in the internal market and repealing Directive 1999/93 / EC and related trust services or regulated, recognized, or approved by relevant national authorities; information obtained by other secure remote or electronic identification processes. (26.4.2019/573). (Laki rahanpesun ja terrorismin rahoittamisen estämisestä 28.6.2017/444.)

If the customer is a foreigner, and does not have a Finnish personal identity number, is it required to also store the information about the nationality and travel documents in addition to the information listed in chapter 3, section 2§ of this law. The notifier is required to inform the customers that the information relating to their identity and other personal data may be used in the prevention, reveling and investigation of money laundering and the prevention of terrorism financing, and to initiate investigation into money laundering and the financing of terrorism, as well as the crime through which the assets or proceeds of the crime is obtained and subject to money laundering or terrorist financing. A customer’s personal information and data gathered for the purpose of

preventing and disclosing money laundering and terrorist financing shall not be used for any other purpose incompatible with the earlier listed purposes. (Laki rahanpesun ja terrorismin rahoittamisen estämisestä 28.6.2017/444.)

In section 4§ of chapter 3 of this law, is the retaining of customer information, the continuous monitoring and reporting obligations discussed. The notifier is required to obtain information on the activities of the customers and the activities of the beneficial owner, quality and scope of the business, and the reasons for using the certain product or service. The notifier is allowed to use the information available on the customer or its beneficial owner from various sources to prepare and maintain a risk assessment of the customer, for the purpose of preventing money laundering and terrorist financing and to fulfil the notification and reporting obligations referred to in this law. The notifier needs to keep in mind and pay particular attention to the credibility of the data source. Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46 / EC (General Data Protection Regulation) and the Data Protection Act (1050/2018) processing of personal data. (26.4.2019 / 573). (Laki rahanpesun ja terrorismin rahoittamisen estämisestä 28.6.2017/444.)

The notifier is required to arrange for adequate monitoring on the quality and scope of the client's activities, the permanence and duration of the customer relationship and the risks to ensure that the customer’s activities are coherent with the experience and knowledge of the customer and its activities. The notifier will need to pay particular attention to transactions that are unusual in structure or size or in the size or location of the notifier. The same is applied if the transactions do not have a clear economic purpose or are incompatible with the experience or knowledge of the notifier about the customer. If necessary, the origin of the funds related to the transaction have to be clarified. (Laki rahanpesun ja terrorismin rahoittamisen estämisestä 28.6.2017/444.)

In section 9 § (26.4.2019/573) in chapter 3 of this law is the exception to the obligation of knowing your customer relating to electronic money discussed. If the notifier considers the risk of money laundering and terrorist financing to be low on the basis of a risk assessment, are the provisions of section 2 of this chapter on customer identification and verification, section 3§ on customer identification and storage and section 4 (1) on customer information not applied. This only being applicable in the case that the following risk management conditions are met; the electronic data carrier is not reloadable or a maximum of 150 EUR per month of electronic money referred to in the Payment

Institutions Act can be deposited on it and the medium can only be used in Finland; a maximum of 150 EUR can be deposited in an electronic medium and can only be used in Finland; the electronic medium may be used only to purchase products or services; the electronic medium cannot be downloaded with anonymous electronic money; the issuer of the electronic media has adequate control methods in place to detect unusual or suspicious transactions. Also, when the maximum of 50 EUR in cash is allowed to be redeemed from an electronic medium, or in the case of a remote payment transaction, the amount paid is not allowed to exceed 50 EUR per transaction. A credit or financial institution may accept a payment from a state outside the European Economic Area (EEA) by anonymous electronic media if the conditions provided for in subsection 1§ above apply to the electronic media. (Laki rahanpesun ja terrorismin rahoittamisen estämisestä 28.6.2017/444.)

Section 11§ of chapter 3 discusses the enhanced obligation of identifying and knowing your customer when identified remotely. If the customer is not present when identifying them and when verifying the identification (remote identification), is the notifier obligated to do the following, to minimize the risk of money laundering and financing of terrorism:

1. By identifying the customer's identity, through gathering additional documents and information related to the identification through a reliable source,
2. To ensure that the payment in regard to a transaction is made for the credit institutions account, or is paid to an account earlier opened in the customer's name, or
3. By verifying the customer through an online identification service or an electronic signature authenticator approved by the law (617/2009) on Strong Electronic Identification and Electronic Trust Services, or through an approved electronic signature, which provides for electronic identification and electronic transaction trust services in the internal market and repealing Directive 1999/93 / EC; (EU) No 910/2014, or through any other electronic identification technology deemed secure, and verifiable. (Laki rahanpesun ja terrorismin rahoittamisen estämisestä 28.6.2017/444.)

Maksulaitoslaki (the law on payment institutions) 30.4.2010/297

This law applies to payment institutions, and in section 1§ of the law, it is discussed how it should be applied. The law should be applied to a business, where a payment service is provided. This law should also be applied to the issuer of electronic money and the electronic money institutions, unless otherwise provided for below. (22.7.2011/899). (Maksulaitoslaki 30.4.2010/297.)

The law 30.4.2010/297 should be applied to the following payment services:

1. A service making a cash deposit to a payment account, or withdrawing cash from a payment account, as well as the management and provisions relating to a payment account.
2. A payment transaction executed through a payment transfer referred to in the law on payment transfers (290/2010), the transferring of money to the service provider's account, as a direct payment or through a payment card, or with any other payment instrument.
3. Issuing a payment instrument.
4. Acceptance and processing of a payment transaction based on an agreement with the payee, which results in transferring funds to the payee; (14.12.2017 / 890).
5. A service, where the service provider receives a transfer from the payer without setting up a payment account in the name of the payer or the payee for the only purpose, to transfer the received transfer to the payee or another service provider acting on behalf of the payee; (14.12.2017/890).
6. Payment initiation service.
7. Account information service; (14.12.2017/890). (Maksulaitoslaki 30.4.2010/297.)

In section 6§ of the law, it discusses the subject of authorization to provide a payment service. A payment service can be provided only if the activity has been authorized in the European Economic Area (EEA) within the meaning of this law. The right to issue electronic money shall be specified in the license of the electronic money institution. (14.12.2017 / 890). The right of a foreign payment institution to provide payment services in Finland is regulated by the law on the Activities of Foreign Payments in Finland (298/2010). (Maksulaitoslaki 30.4.2010/297.)

The section 9 a § in chapter 2 of this law states that a payment institution providing payment accounts shall provide an account transfer service to consumers and report it to the Financial Supervisory Authority in accordance with Chapter 15a, Sections 2§ to 7§ of the law on Credit Institutions (Maksulaitoslaki 30.4.2010/297).

In section 39§ under chapter 6, the knowing your customer is discussed. According to this law is the payment institution required to know their customers. The payment institution is required to identify the beneficial owner of the customer and the person acting on behalf of the customer, as well as verify their identity, when applicable. The payment institution is not allowed to offer their customers an anonymous account. When fulfilling the obligation stated in this subsection, are the systems referred to in subsection 2§ to be utilized. (1.6.2018 / 409). The payment institution is required to have adequate risk management systems in place, to assess the risks posed by the customers, of the institutions operations. Also are the provisions of the law on the Prevention and Investigation of Money Laundering and Terrorist Financing applied to the customer knowledge. The Financial Supervision Authority is allowed to issue more detailed regulations on the procedures to be followed in knowing the customer referred to in subsection 1§ and on the risk-management referred to in subsection 2§. (Maksulaitoslaki 30.4.2010/297.)

Maksupalvelulaki (law on payment services) 30.4.2010/290

The scope of application of this law is discussed in section 1§ in this law, which is the obligation to provide information and the terms and conditions regarding the services, as well as regarding the implementation of payment services. The 30.4.2010/290 is applied to the following payment services:

1. A service making a cash deposit to a payment account or withdrawing cash from a payment account and activities related to the management and provision of a payment account;
2. Execution of a payment transaction by account transfer, transfer of funds to the service provider's payment account, direct debit or by payment card or other means of payment;
3. The issuance of a payment instrument;
4. Acceptance and processing of a payment transaction based on an agreement with the payee, which results in the transfer of funds to the payee;
5. Money intermediation;
6. Payment order service;
7. Account information service. (Maksupalvelulaki 30.4.2010/290.)

Payment services where a payment transaction is executed with a payment card are further regulated by Regulation (EU) 2015/751 of the European Parliament and of the Council on transfer prices for card-based payment transactions, further in the document "the Regulation on transfer pricing for card payments" (29.1.2016 / 59) (Maksupalvelulaki 30.4.2010/290).

3 Research Methods

In this chapter, the research method used, as well as the data sourcing is discussed. The way the information will be collected, and further the risks and limitations as well as the reliability and validity relating to this thesis will be discussed in this chapter.

The research method used for this thesis is called the mixed method, meaning both the qualitative as well as the quantitative research method was used.

Qualitative approach
The qualitative method has been used when looking at the different banks' websites and apps, as well as making comparisons between the findings of the different service providers, making the app providers websites the primary source for the qualitative research. The qualitative nature of the study therefore aims at describing the user experience from a personal point of view of the author and uses the standard comparative reasoning approach often employed in qualitative research. Qualitative data about the bank characteristics is obtained from a range of internet sources and summarized, but its contribution to the whole thesis is of such minor nature that it is not included as a formal part of the Research Design. In addition, interviews were conducted with financial business experts to collect information about the ongoing and predicted future changes in the banking industry arising from the entry of Neobanks.

Quantitative approach
The quantitative approach was taken when looking at the market shares, the number of customers, and by looking at the added value the Neobanks have provided their customers, the numeric data regarding cybercrime, as well as the numeric data differentiated by different industries and types of cybercrime. A quantitative approach for the research was also taken when looking for and analysing the numeric data gathered through websites and previously existing statistics about the Neobanks, more specifically the percentages of age categories of Neobank users.

3.1 Data Sourcing and Collection Methods

The author made a market research on what Neobanks are available, and through Statista's website the author chose the two biggest in Europe. The decision regarding traditional banks was made as follows, two bigger ones and one smaller bank in Finland. The traditional banks were chosen through a statistic provided by the Bank of Finland, on the Finnish traditional banks' market share. The credit institutions, FIN-FSA, as well as the

law regulators and governments own website's, were used as sources for the information needed for this thesis. Statistical websites, and globally acting consulting companies in the field of technology and finance.

The primary and secondary data in this thesis has been sourced through numerous channels. Regarding the empirical study data were systematically sourced from the selected bank websites and apps. Further primary data were collected through interviews with professionals of the banking and credit industry. Additional secondary data for the theoretical part were collected from the authority's websites, legislative websites, such as Finlex, where all Finnish laws can be found, as well as FIN-FSA, which is the website where specific regulations can be found regarding banks and credit institutions. Finally, also the EU regulators website regarding regulations set in place for EU member states, as well as UK governmental websites for the sourcing of laws and regulations, were used as data sources for the theoretical part of the thesis.

3.2 Data Analysis

The thesis presents a comparative analysis of all the phases of customer registration and usage process, identifying the differences and lack of steps in registration process and mapping them according to Table 1. Additionally, the in-depth interviews of the financial experts are similarly analysed to reflect the investigative questions.

3.3 Risk and Limitation

Potential risks and limitations stem from the risk that the chosen banking operators are not representative enough for the market. However, since the chosen banks have the largest market shares, they are considered to offer a robust view of the Neobanks operations compared with the traditional banks. Other risks within data collection, is the availability of academic information, since the Neobanks are new players on the market, and therefore have not yet gained much interest in academic research. Due to the possibility of the information sources, and the data collected from internet sources not being academically based, can the reliability and validity of the information collected be more biased. However, to minimize the risk of incorrect information, the author chose to mainly use sources that represent credible international consulting companies.

3.4 Reliability and Validity

Since the chosen banks have the largest market shares, they are considered to offer a robust and valid view of the Neobanks' operations compared with the traditional banks.

The secondary data sources used for the theoretical part represent public legislative documents and can thus be considered reliable.

4 Neobanks, a Change to the Banking Industry

Throughout this results chapter, the author will discuss and compare the results received through the research conducted. We go through the banks websites and apps, as well as take into account the risk that could possibly be encountered through the usage of these Neobanks, as well as look at the research results of the legal and legislative aspect regarding banks and credit institutions. Finally, we present the perspectives of interviewed field professionals, regarding their assessment of Neobanks vs. the traditional banks in the last subchapter 4.5.

4.1 Customer Experience

Customer experience is a central part of the decision-making in what service provider someone chooses, such as their bank. The customer registration process being a very important part of the customer experience from the perspective of customer on boarding and retention. Contemporarily, many customers expect that everything should be as fast, simple and transparent as possible. But especially in the banking industry, the AML and KYC perspectives being extremely important and the requirement to follow laws, bring the need to balance them with the customer experience. Through the next subchapters we will look into the registration process of the traditional banks, and the registration process for the Neobanks, the process which has been tested and reviewed by the author.

Customer Registration Process in Traditional Banking

The customer registration process of traditional banks in Finland may differ between banks, but they all have to follow the guidelines enforced by FIN-FSA and the Finnish law. You are usually able to fill in the customer registration application online, but only regarding some of the services. Some banks may require a visit to their branch, to be identified and get identifiers, before being able to open an account, or apply for a loan online through the webbank.

The banks who accept applications online, require that you have bank codes from another Finnish bank, but they may not accept all Finnish bank codes, and they also require you to have a passport or ID card. You are required to have a Finnish phone number, when becoming a customer in a Finnish bank. You are also required to have a Finnish social security number, as well as a Finnish address. To fill in the application online, you should also be of age. (Nordea 2020a.)

A very important new regulation put in place in the beginning of 2018 is that a driver's license is not accepted as identification in a bank when opening a bank account and receiving your bank codes. These bank codes can be used as identifiers in other official matters in Finland, making it more important to be certain that the person using them is exactly who they claim to be. Because the driver's license is no more overseen by the Police, is it not a valid identification method in these matters. Making these matters stricter, is embedded in the money laundering and anti-terrorism act.

Banks are required to know their customers according to the money laundering and anti-terrorism act. The "know your customer", also known as KYC, is an EU regulation, requiring banks to ask their customers certain questions, such as the financial life situation, the intentions of the bank services, the source of funds and assets, an estimation of cash deposits and withdrawals, as well as estimations of international payments into or from your bank account. The questions also include whether you, or if anyone of your family members or close business associates are entrusted with a prominent public function, as well as what your liabilities are to foreign countries, a politically exposed person. (OP 2020.)

Customer Registration Process in Neobanks

The customer registration process for Revolut and N26 are very similar in the steps needed to be taken to become a customer. The registration process tested by the author went according to the following.

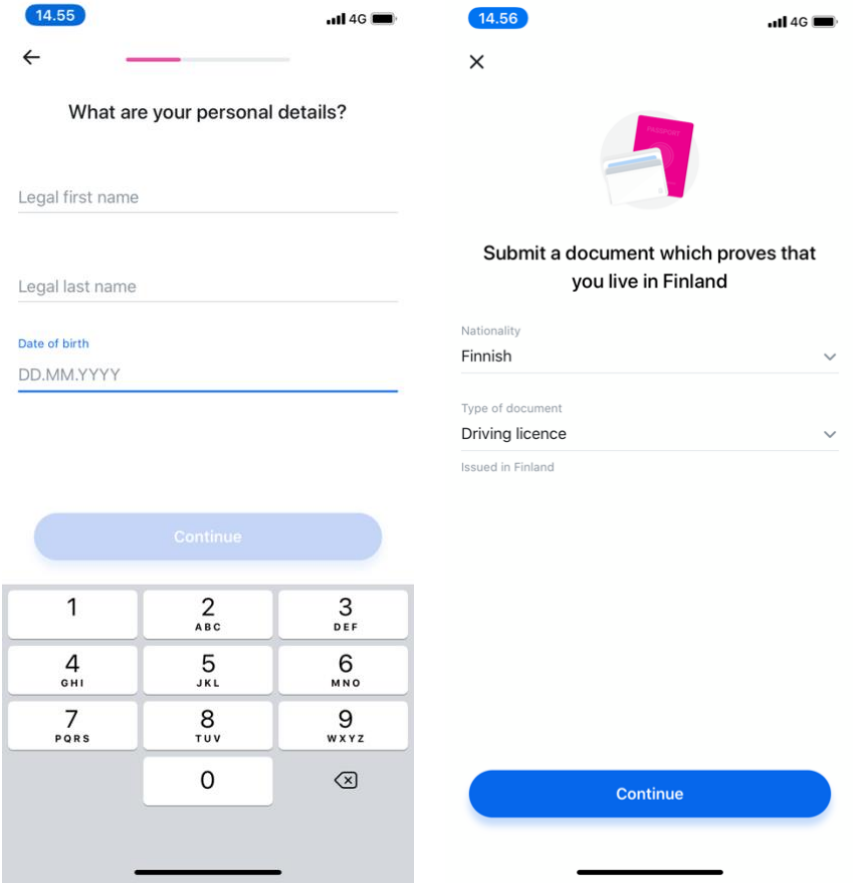
The customer registration process of Revolut:

When applying to become a customer and open an account at Revolut, the process goes as follows according to the authors testing conducted on 28th August 2020.

Firstly, you need to enter your phone number, after which the application asks you to create a passcode for the Revolut account, and after this you will be sent a code which you've received as a text message to the phone number entered in earlier. Then you are requested to fill in your personal details, your legal first and last name as well as date of birth. Then you will be asked to fill in your home address, country street address, postal code as well as city. Then you are asked to fill in your email address and tell them your main reason for using Revolut, choosing between the options of, spending or save daily, spending while travelling, send money, or gain exposure to financial assets. Then you will

have to submit a document that you live in the country you have earlier told them you live in. It asks your nationality and to select the type of document you will be submitting, driving licence, ID card or passport. Finally, you will be requested to take a selfie so that they can match your selfie to the photo on the document submitted. After this you will be able to choose between a physical card and a free virtual card as well as start using your services. The account opened is registered with the Revolut Payment UAB entity. We discuss further the deposit protection according to which registered entity the account is registered with later in this chapter.

Picture 1. Revolut, what are your personal details and submitting an identification document. 2020.



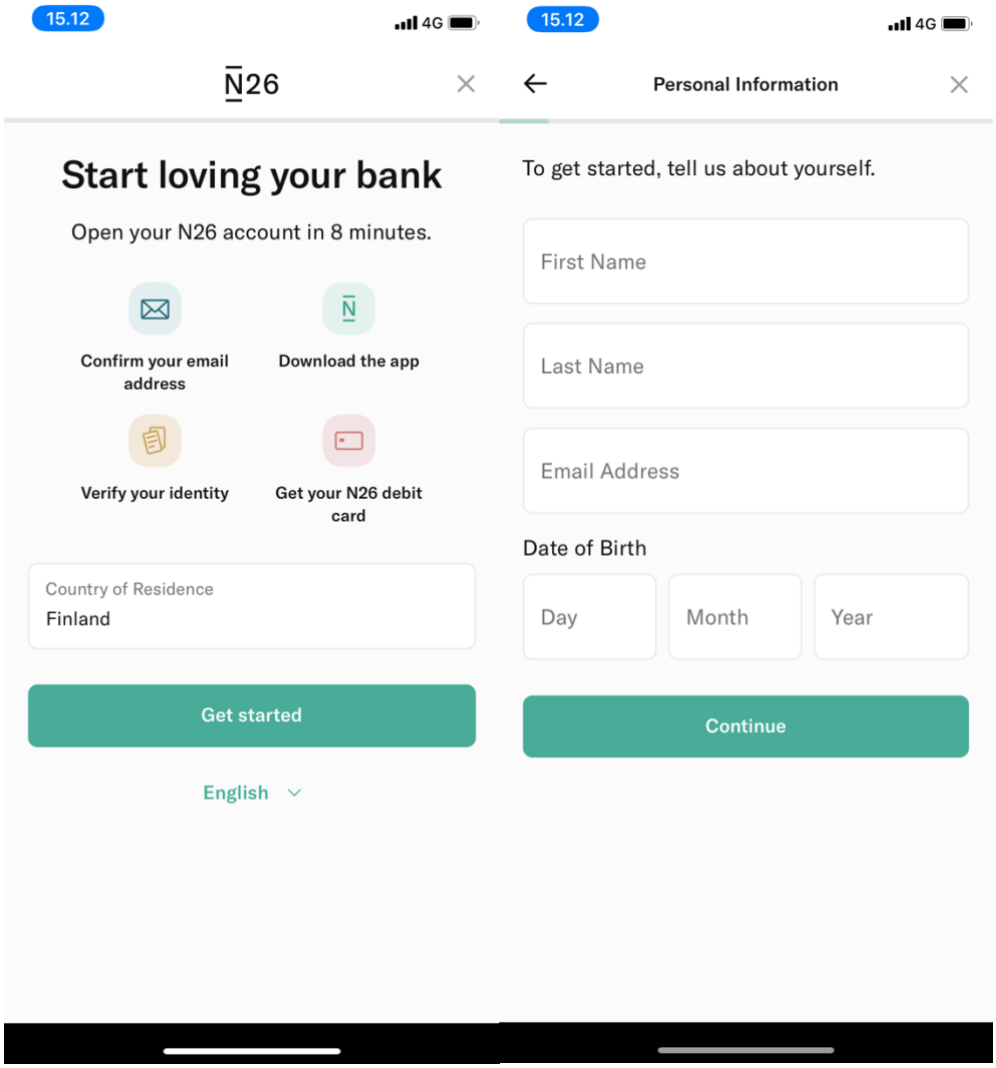
The customer registration process of N26:

When applying to become a customer and open an account with N26, goes the process goes as follows according to the authors testing conducted on 28th August 2020.

Firstly, you need to choose your country of residence, after which you will fill in your first and last name as well as email address and date of birth. After this you will be asked to fill in your phone number and your address where you want your N26 card to be shipped. Then you are asked to fill in your nationality, city of birth, the country of birth as well as your legal sex, female or male. Then you will be requested to fill in if you are also a U.S. citizen or green card holder, and then if you are subjected to tax in the U.S., and in which country you are tax liable. N26 is required to inform the Organization for Economic Co-operation and Development (OECD) of certain tax information according to the Common Reporting Standard. Therefore, N26 needs to know in which country you are tax liable in. (N26 2020a.)

Then you will be requested to create a password, and to agree to the Terms & Conditions (see appendix 4) as well as their privacy policy. Then you will be asked to check your email and verify your email address. Then you are asked if you will be using your account for business purposes or personal use only. Then you will be able to choose your plan between Metal, You, and Standard, after which you will be sent an SMS to the phone number you've filled in earlier. Finally, you are asked to verify your identity, either through an ID card or a passport, through taking photos of your identification document as well as a picture of your face to match to your picture on your identification document. After these steps you are done and by setting your confirmation PIN you can start using your account.

Picture 2. N26, start loving your bank and personal information. 2020.



When looking into the main difference between the two Neobanks N26 and Revolut, we can see is that Revolut allowed you to sign up with your driver's licence as a form of identification, which N26 does not accept as a form of identification. N26 also asks you to fill in the city as well as country of birth, which Revolut does not do, and which necessarily might not be seen on a form of identification. N26 also asks your legal sex, if it is male or female, which Revolut does not. Revolut neither asks if you are a US citizen or green card holder, nor if you are subjected to US tax or in which country you are liable to pay taxes.

When comparing the customer registration process of these two Neobanks to the customer registration process of the traditional banks, the biggest difference is due to the fact that traditional banks have to strongly identify you at a branch, if you do not have Finnish banking codes.

According to the Basic pre-contractual information of N26, is the deposit protection fund of their customers with the Entschädigungseinrichtung deutscher Banken GmbH (German Banks Compensation Scheme). The limit of the deposit protection is 100 000 € and is applicable to each depositor (Appendix 3). N26 is applicable to German law and in the jurisdiction of Federal Republic of Germany. In order to open an account, you are required to have a smartphone as well as a phone number. You are required to agree with N26s' terms and conditions as well as consent to a credit check. (appendix 2.)

According to the account terms and conditions is N26 required to identify and verify the customers identity according to law. The customer is required to inform N26 of data regarding their name, address, date of birth, phone number as well as the e-mail address, as well as immediately inform N26 any changes regarding this data. (appendix 4.)

According to the Revolut article "Is my money safe?" is the customer's money safeguarded depending on the entity the customer is registered to. If the entity is the Revolut Payment UAB, is the customers money safeguarded by Revolut holding the customer's money in a separate account within the credit institution. The isolated account with the customer's money, is held by Revolut on behalf of the customer. This protects the customer in the case of Revolut going bankrupt, since the customer will be able to claim their money from the isolated account and will also be paid before other creditors. Due to the fact that the account which the customer has with Revolut, is an electronic money account instead of a bank account, is the customer's money not guaranteed by the Lithuanian deposit insurance administered by the State Enterprise Deposit and Investment Insurance. (Revolut 2021a.)

In case the customer's account is registered under the Revolut Bank UAB and Revolut Payment UAB entity, is the customer's money insured by the Lithuanian State Company, Deposit and Investment Insurance, as a single depositor up to 100 000 €. In case the customer's account is registered under the Revolut LTD entity, is the money protected, since Revolut safeguards the customer's money in a separate client account in one of the large banks Revolut has client accounts with. Since the customer's account is an electronic money account, and not a bank account, is the customer's money not protected by the Financial Services Compensation Scheme. (Revolut 2021a.)

The Personal terms of the Revolut account, for a Finnish account holder, is under the terms and conditions of Revolut Payment UAB. In these terms and conditions is open banking, making payments and accessing the customer's own account stated. According

to the terms and conditions, can the account holder access accounts which they have with other banking service providers, through the Revolut app, as well as give permission for the other banking service provider to access their Revolut account. The open banking providers given access to the customer's account, can then make payments on the customer's behalf, but must usually be authorised by a regulator such as the Bank of Lithuania, to do so. In case of concern of fraud, must Revolut block the access by the open banking provider. (Revolut 2021b.)

Mandatory consumer protection rules of the EEA country the account holder lives in, as well as Lithuanian law applies to the terms and conditions, and agreement, which the Finnish account holder has with Revolut. In case legal action is taken, can it under the terms and conditions only be brought in the courts of the Republic of Lithuania, or any EU Member States court, in which you have the statutory right to bring legal action, under the terms and conditions. (Revolut 2021b.)

According to the basics of cryptocurrency, you can use the Revolut app to either buy, sell, or receive cryptocurrency, or then send cryptocurrency to another account with Revolut. Cryptocurrency is not deposit protected under Financial Conduct Authority, nor the Financial Services Compensation Scheme. Revolut might limit the amount of cryptocurrency the customer can buy, which they will let the customer know, before Revolut accept the customer's instructions on the buy. The customer is able to transfer cryptocurrency to anyone in the Revolut app, or anyone who isn't a customer with Revolut. (Revolut 2021c.)

Risks related to cryptocurrencies, can be very significant. Like anything else digital, is there the risk of it being hacked, altered, or affected by technical problems. This might result in a delay of selling, transferring, or spending your cryptocurrency, or in the worst-case scenario, loose your cryptocurrency. The lack of regulation on cryptocurrency can change at any time, which would affect the value of the cryptocurrency, and fall. This would be more likely in the case of cryptocurrency, then with normal fiat money. The fall in value might also happen due to a new better cryptocurrency being created, or if a software developer makes a change to the cryptocurrency and how it works unexpectedly. (Revolut 2021c.)

4.2 Banking Services Offered According to Bank

Through this subchapter the author goes through banking services that the banks being researched in this thesis provide to their customers. The banks researched in this study, as the traditional banks are Danske Bank, Nordea, and S-Pankki. The Neobanks that have been chosen for this research, are Revolut and N26. When looking at Danske Bank's, Nordea's, and S-Pankki's websites, you can clearly see already at the first glance that they offer much more services than Revolut and N26. In the table below, you can see a condensed overview of the services the chosen banks provide, and the broad difference and variety in the service selection.

Table 1. Banking services differentiation table. 2021.

	Danske Bank	Nordea	S-Pankki	N26	Revolut
Basic Banking Services					
Bank accounts	x	x	x	x	x
Bank cards	x	x	x	x	x
Debit	x	x	x	x	x
Credit	x	x	x		
loans	x	x	x		
Saving and Investment					
Funds	x	x	x		
Stocks	x	x			x
Bonds & structured Bonds	x	x			
ETFs	x	x			
Insurance saving	x	x			
Online banking services					
Webbank	x	x	x	x	x
Apple Pay	x	x		x	x
Google Pay	x	x		x	x
Mobile Banking App	x	x	x	x	x
Identification App	x	x			
E-invoice	x	x			
Payment services	x	x			
E-payments	x	x	x		
Foreign currency payments	x	x		x	x
Customership plans					
Basic	x	x		x	x
standard	x	x		x	x
Premium	x	x		x	x

When looking at Danske Bank's website, you see that the products they offer range from different bank accounts, to different card options, to different saving and investing products. The same goes for Nordea's website, as well as S-Pankki. While looking at Revolut's website you can only see that they offer a bank account, with different card

options, and currency and stock trading. With the N26 website, you can see that they have even less products or services listed, they offer different accounts and different cards, but nothing else.

Danske Bank

According to danskebank.fi website, Danske Bank offers Target loans, One-Time loans, Consumer loans, Student loans, and ASP loans. They also offer different bank accounts, Danske account, which is for handling day-to-day financing, Danske target account, which is for saving for a dream or goal. Danske benefit account, which is for depositing funds, Danske safety account, which is mainly for saving for emergencies. The Danske golden piglet account is meant for a child's first account, and the ASP account, which is for saving for your first home. (Danske Bank 2020.)

Danske Bank also offer different benefit programs, Danske Study, Danske youth, and Benefit level 1 to 4. Through these programs, you can gain access to their different everyday service packages, these are Danske silver, Danske gold, and Danske Platinum Plus. Danske Bank offers six different card options, Platinum, Gold, Silver, Debit Student, Credit/Debit K-plussa, Finnair Plus Visa. (Danske Bank 2020.)

In addition to these products, Danske Bank, also offer Saving and investment products and services. The section includes, Funds, Stocks, Bonds and structured bonds, ETFs, Insurance saving, with MIFID 2 level service. (Danske Bank 2020.)

In addition to the above-mentioned products and services, Danske Bank also offers online banking services, webbank, Apple pay, Google pay and a Mobile Banking app, through which you can make payments, transfer money between your accounts, trade and invest, monitor your loans, as well as oversee your cards and manage the cards restriction areas, limits, as well as close or re-open your card. Through the app you can also reach out to customer service, as well as accept e-payments. They also offer an app called Danske ID, which is in according to the new law which came in effect in the fall of 2019. Through this app you can identify yourself when login into online platforms as well as your webbank. (Danske Bank 2020.)

Nordea

According to Nordea.fi website, they offer the following services: Accounts and payments, credit and debit payment cards, loans and consumer loans, saving and investing, insurance, and customer benefits. (Nordea 2020). Accounts and payment services Nordea offers, are disposal accounts, e-invoice, foreign currency payments, e-payments, rental security deposit account, epiggy, credit transfer, payment services, currency payments, SEPA direct debit, SEPA instant credit transfer. Credit and payment cards Nordea offer, credit cards: Nordea gold, Nordea credit, Nordea premium, TUOHI Mastercard, Finnair Plus Mastercard, Stockmann Mastercard. Debit cards: Nordea debit, Nordea Visa Electron. (Nordea 2020.)

Loans and consumer credit Nordea offer are Home loans, such as Loan promise, Housing Loan, Green housing loan, ASP loan, HomeFlex. Consumer credit that Nordea offers, Flexicredit, Car loan, Travel loan, Secured consumer credit, student loan. The saving and investment services Nordea offers, are Funds, Equities, Online trading, Savings account, Saving and investment products, sustainable saving and investing, Monthly saving, as well as Saving for your children. The service you get from Nordea is also in par with the MIFID 2 directive. (Nordea 2020.)

Through your Nordea customer ship, you get discounts on your Insurance as If. The insurances are Home insurance, Vehicle insurance, Boat insurance, Children’s insurance, Travel insurance, Forest Insurance, If You Young Customer’s insurance, as well as Horse insurance. (Nordea 2020.)

Nordea also offers different benefits, such as benefits for premium customers, benefits for housing loan customers, benefits in your daily banking, and benefits for student customers. Nordea also offers different online and mobile services, such as Nordea mobile app, Nordea Code app, Netbank, Access codes, Apple pay, Google pay, Nordea Wallet, Siirto, as well as meniga rewards. (Nordea 2020.)

S-Pankki

According to S-Pankki.fi website, S-Pankki offers services to their customers, such as, accounts and webbank services, cards, loans, saving and investing, as well as insurance services. (S-Pankki 2020.)

S-Pankki only offer one account, called an S-account. Cards that you can link to your S-account, are debit- and credit cards, S-Benefit card Visa Credit/Debit. S-Pankki also offer different type of loans, Housing loans, S-loan, as well as credit. As an S-Pankki customer you can also invest through funds, S-funds and FIM funds. You are also able to get a discount on Lähitapiola's insurance, as well as receive bonuses through your S-Pankki customer ship.

Your S-Pankki card doubles as a benefit card for the S-groups benefit program. The bonuses you receive from your purchases, using your benefit card, will be credited to your S-account. S-Pankki also offers in addition to their webbank, a mobile application, through which you can manage your accounts and cards, track and manage your saving. You can also manage your investments, as well as your loans. You are also able to easily buy Lähitapiola's insurance, and report on damages when needed.

N26

According to the N26 website, the N26 Neobank offer three different customer ship plans, N25 Standard, N26 You, and N26 Metal. The N26 Standard package offers you a free German bank account, which includes a debit MasterCard, free payments worldwide in any currency, up to 3 free withdrawals in the Eurozone, up to 2 sub accounts, as well as a deposit protection up to 100 000 €. Their second account package the N26 You, includes a free German bank account, a free debit MasterCard, free payments worldwide in any currency, up to 5 free withdrawals in the Eurozone, unlimited free ATM withdrawals in any currency, medical travel insurance, trip insurance in case of cancelations, flight insurance in case of delays, luggage coverage in case of delay or loss. This package also includes mobility insurance for shared vehicles, winter sport insurance in case of accidents. This packing also includes up to 10 sub-accounts, shared sub accounts with up to 10 N26 users, as well as partner offers, as well as a deposit protection up to 100 000 €. The only customer service you will receive with these customer ships, is a 24/7 chatbot assistance, and a in live chat possibility with a specialist. (N26 2020.)

The third customer ship package N26 Metal includes a free German bank account, a metal debit MasterCard, free payments worldwide in any currency, up to 8 free withdrawals in the Eurozone, unlimited free ATM withdrawals in any currency. It also includes the travel insurance package, medical travel insurance, trip insurance in case of cancelations, flight insurance in case of delays, luggage coverage in case of delay or loss. Other insurances included are mobility insurance for shared vehicles, winter sport

insurance in case of accidents, car rental insurance when away from home, and phone insurance for damages and theft. This packing also includes up to 10 sub-accounts, shared sub accounts with up to 10 N26 users, as well as partner offers, as well as benefits selected access benefits and rewards. The deposit protection is also up to 100 000 €. Through this package are you able to receive not only the 24/7 chatbot assistance, and a in live chat possibility with a specialist, but you have access to a dedicated phone line. (N26 2020.)

Revolut

Revolut offers three different customer ship plans: standard, premium, and metal, according to the website. The standard customer ship package includes a free UK bank account, a free Euro IBAN account, the possibility to spend in over 150 currencies at an exchange rate at the interbank exchange rate, and exchange in 30 flat currencies up to 1 000 € a month. They offer ATM withdrawals up to 200 € a month without any fees, a free Revolut card, instantaneous access to 5 different cryptocurrencies, one Revolut Junior account for a child, as well as one cross boarder transfer for free per month. (Revolut 2020.)

The second package they offer is the premium package, which includes a free UK bank account, a free Euro IBAN account, the possibility to spend in over 150 currencies at an exchange rate at the interbank exchange rate, and exchange in 30 flat currencies without a monthly limit. They offer ATM withdrawals up to 400 € a month without any fees, overseas medical insurance, insurance on delayed baggage and delayed flights, a winter sport coverage, global express delivery, instantaneous access to 5 different cryptocurrencies. You'll receive a premium card, disposable virtual card, Lounge Key pass access, free lounge passes for you and a friend if your flight is delayed by more than one hour. You will also get access to two Revolut Junior account for two children, as well as one free SWIFT transfer per month, and an unlimited amount of cross border transfer. You will also get access to priority customer support when needed. (Revolut 2020.)

The third customer package offered is the metal one, which includes a free UK bank account, a free Euro IBAN account, the possibility to spend in over 150 currencies at an exchange rate at the interbank exchange rate, and exchange in 30 flat currencies without a monthly limit. They offer ATM withdrawals up to 800 € a month without any fees, overseas medical insurance, insurance on delayed baggage and delayed flights, a winter sport coverage, purchase protection, car hire excess and global express delivery. You will

also receive an instantaneous access to 5 different cryptocurrencies, an exclusive Revolut Metal card, disposable virtual cards, Lounge Key pass access, free lounge passes for you and up to three friends if your flight is delayed by more than one hour. You will also get access to five Revolut Junior account for five children, 0,1% cashback on card purchases made in Europe, and 1% cashback on card purchases made outside of Europe. Lastly, you'll receive one free SWIFT transfer per month, and an unlimited amount of cross border transfer. You will also get access to priority customer support when needed. (Revolut 2020.)

4.3 Challenges and Risks Associated with Neobanks

With the fast and steady development in the technological industry, risks associated with the industry have been rising alongside the industry itself. One big risk associated with the technology in the financial sector and the banking industry is cybercrime, which has been increasing dramatically according to the research conducted by Accenture in 2019. (Accenture 2019.) According to the same study, has the expense of the cybercrime against the financial sector increased steadily. There is risk in innovation and growth according to the study conducted by Accenture. This factor has to be taken into consideration when looking at the uprising Neobanks which are rapidly becoming more popular.

According to the earlier mentioned study, Accenture found that there was a significant increase in cybercrime from the average number of security breaches in 2017 (130), to the average number of security breaches in 2018 (145), resulting in an 11% increase during the year, and in total in a 67% increase during the last five years. This study also found that the increase in cost of cybercrime, went up from 11,7 million dollars as an average cost of cybercrime in 2017 to 13,0 million in 2018. This makes the increase 12% from the year 2017 to 2018, and a 72% increase during the last 5 years. These numbers should be very alarming, especially to the banking industry which according to the study, continued to have the highest cost of cybercrime share with the utilities industry. The average annual cost of cybercrime for the banking industry in 2017 was 16,55 million US dollars but made a drastic rise to 18,37 million US dollars in 2018, as seen in the figure down below.

BENCHMARKING CYBERSECURITY INVESTMENT

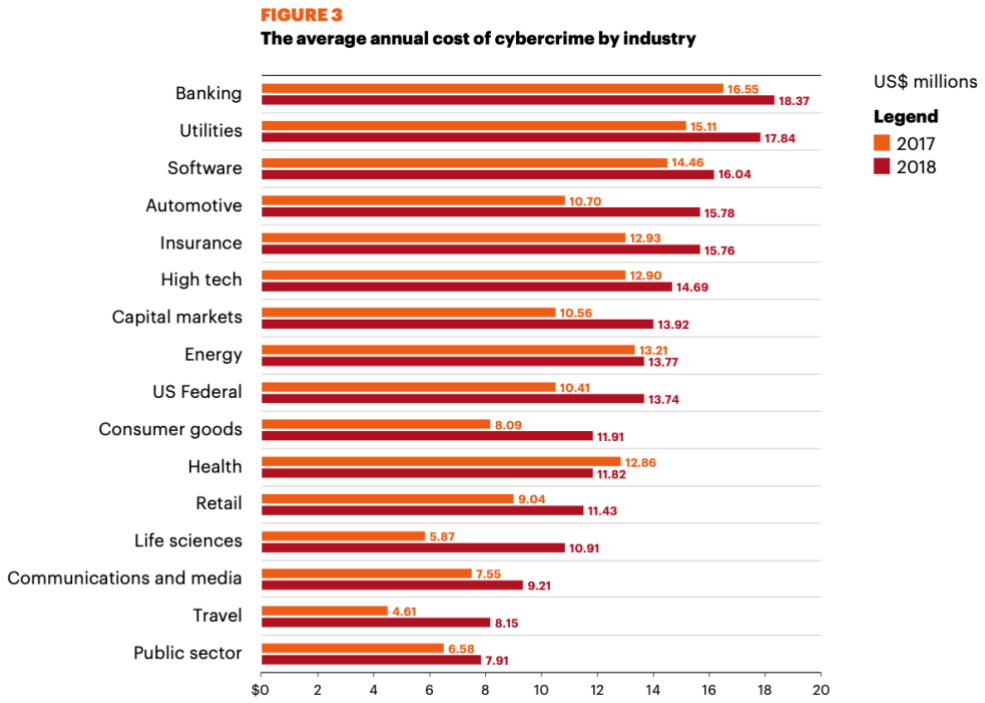


Figure 7. The average annual cost of cybercrime by industry (Accenture 2019.)

The risks the drastic growth in cybercrime impose, is a significant risk on customer data and information. Regulations such as General Data Protection Regulation (GDPR) is meant to enforce customer information and data protection and make companies much more aware and responsible of the customer data they keep. (Accenture 2019.)
As shown by Figure 8 below, the different types of cybercrime attacks can cause different type of cost full damage, business disruption, information loss, revenue loss as well as equipment damage. The two biggest types of cybercrime attacks malware, and web-based attacks, cause over all most cost consequences in the area of information loss.

FIGURE 8
Consequences of different types of cyberattacks
(average annual cost; figures in US$ million; 2018 total = US$13.0 million)

	Business disruption	Information loss	Revenue loss	Equipment damage	Total cost by attack type
Malware (+11%)	$ 0.5	$ 1.4	$ 0.6	$ 0.1	$ 2.6
Web-based attacks (+17%)	$ 0.3	$ 1.4	$ 0.6	$ –	$ 2.3
Denial-of-service (+10%)	$ 1.1	$ 0.2	$ 0.4	$ 0.1	$ 1.7
Malicious insiders (+15%)	$ 0.6	$ 0.6	$ 0.3	$ 0.1	$ 1.6
Phishing and social engineering (+8%)	$ 0.4	$ 0.7	$ 0.3	$ –	$ 1.4
Malicious code (+9%)	$ 0.2	$ 0.9	$ 0.2	$ –	$ 1.4
Stolen devices (+12%)	$ 0.4	$ 0.4	$ 0.1	$ 0.1	$ 1.0
Ransomware (+21%)	$ 0.2	$ 0.3	$ 0.1	$ 0.1	$ 0.7
Botnets (+12%)	$ 0.1	$ 0.2	$ 0.1	$ –	$ 0.4
Total cost by consequence	$ 4.0	$ 5.9	$ 2.6	$ 0.5	**$ 13.0**

Figure 8. Consequences of different type of cyberattacks (Accenture 2019.)

Hacking is a great potential risk in today's world of online services. The risk of an outside source getting their hands on your money and investments by hacking into your bank account. Depending on how vulnerable your bank is, depends on how big the risk of this happening is. According to a study done by ImmuniWeb, there were only three banks out of the 100 included in their research, that got a ranking of A+ on their website security. (ImmuniWeb 2019). Of course, this is also a risk for the banks, since in the case hacking would happen, they would lose their reputation, which is one of the hardest things to build back again.

Cyber-attacks in the banking industry

In 2016 Vincent Haupert showed how the Neobank N26's data could be exposed and then accounts hijacked by hackers. User credentials to almost 33 000 users were requested from N26's own software feed. The Anti-fraud systems set in place to prevent this, were not able to detect the exposure. This shows the importance of technological companies to stay ahead with their software systems, and their Anti-fraud systems. (Ghosh, A. 2019.)

A recent risk for customers of Neobanks is linked to the COVID-19 pandemic surging through the world in 2020. The pandemic has affected people's income drastically, during 2020 the estimated employment income level dopped by 5,2% compared to 2019. (Eurostat 2020.) Due to the sudden need for loans, and people needing to stop their repayment of their loans, banks had to keep focus only on their existing customers. Due to this, traditional banks had to turn away loan applications by people and companies which

did not have an already existing customer relationship with them. For a customer relying solely on a Neobank, would this be a risk, since most general Neobanks do not offer any credit or loans.

Onboarding Risks in Banking

A big risk with Neobanks, is that they attract people who commit fraud, due to the onboarding process being particularly vulnerable. Money launderers wish to be able to open an account, through which they would then be able to launder their money. The people wanting to commit fraud may also want to be able to convert their funds to cryptocurrency, which they would be able to do through the Neobank acting as a middleman for the exchange. Another type of scammers wanting an account with a Neobank, are the ones trying to scam people out of money when having a legitimate looking bank account through which they can receive deposits, for the promised service or product which then will never arrive. The Neobanks could lose their extremely valuable reputation, as well as might get fined by regulators. (Florian 2021.)

One big risk regarding the onboarding process, is the risk of people committing fraud, opening an account with a stolen or fake identity. Online fraud being mostly linked to stolen ID's, which can be bought on online in bulk for the purpose of opening an online bank account. Personal data also being gathered through phishing, fake job application or through hacking. Online fraud can also be committed through the use of a synthetic ID, which is combined by real and fake personal information. The popular growth in AI technology in today's world has brought new technology as deepfakes. Deepfakes being videos or audio recordings of a person digitally created without someone's permission also represent a risk for the onboarding process. (Florian 2021.)

Some suggested steps, which Neobanks could take, to identify their customers more securely. They should especially take extra steps by analysing if the email address or phone number has recently been created, and if they are used for any social media accounts. Checking the IP address, if the person is using a virtual private network (VPN) which encrypts the data as well as hides the IP address and location, or if the person is using a public network. They should also look at the data, regarding if the person is using an emulator masking the original computer system they are using, or if the device the person is trying to login with looks to be real. (Florian 2021.)

4.4 Neobanks Relation to Banking Law and Regulation

Through this subchapter will the author discuss shortly some thoughts and reflections regarding Banking laws and regulations and their relations to Neobanks.

Laws have been changed to being more progressive, which has then enabled the Neobanks to emerge to the market. For example, a Finnish citizen can acquire a bank account with Revolut, and the bank account is then a British bank account. There is no technical branch in Finland, meaning that Revolut does not have to comply with Finnish law, Finnish Financial Service Standards and is not overseen by FIN-FSA, the Finnish Financial Supervisory Authority.

According to Finnish law and European regulation are banks required to know if their customers are a politically exposed person, or e.g., related to one. This can be checked through certain systems, but most banks also ask their customers that specific question. Neither Revolut nor N26 asked the author, when signing up with their services, if the author was a politically exposed person (PEP). They are according to law required to check if their customers are a PEP, and in case the customer is a PEP conduct an enhanced customer due diligence. Since they did not ask the consumer about the PEP person status, they are neglecting an important aspect of the KYC principle.

4.5 Interviews

In this subchapter we will look into the interview answers of two professionals in the field. Through the interviews conducted, have the professionals in the field confirmed findings of this thesis. The first interviewee, further referred to as “Expert A”, is a CEO of a major financial institution operating in the Nordic region. The second interviewee, “Expert B”, is a director of a department at a major financial institution, with broad expertise of e-payment solutions. Both interviewees have solid expertise in online banking and payment solutions, both of which are focus areas of this thesis.

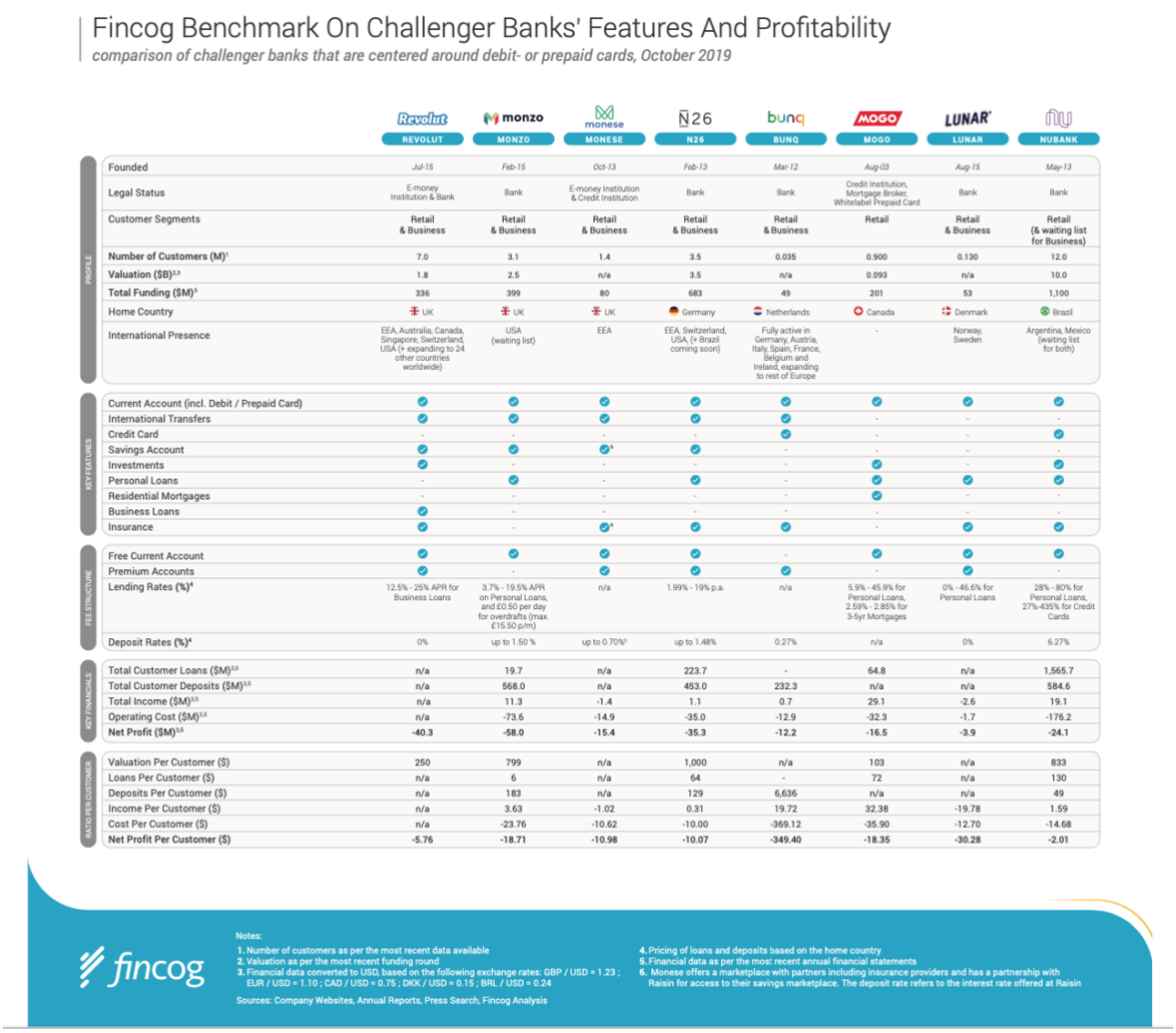
The most relevant point to this thesis, which both professionals pointed out in their interview answers, were that there is a clear need for the traditional banks to make a change in their business practices to keep up with the uprising Neobanks in the future. The problem which arises for the traditional banks, is their big legacy systems, due to which they are not able to just automize and digitalize many of their processes, meaning they will not be able to make any fast and drastic changes. The traditional banks need not (yet) be too worried about this, since they still have the position as the primary bank of

most customers, as well as the existing history. The traditional banks also have the advantage of the loans they provide to the customers, creating an extensive grip on the customers. In conclusion is the understanding of both the author, Expert A and Expert B, that the traditional banks need not to be concerned about the short-term future and would not even be able to make fast drastic changes, but that they have to start changing to be able to compete on the same level longer into the future.

When asking Expert A and Expert B on what they think will be the leading business model in the banking sector in the near future within a 5-year time frame, they had both very valid remarks, but from two different points of view. Expert A commented that the freemium business model will probably be where the consumer market will be turning towards. The freemium business model is when there is a free offer, and then there is a disruption or friction introduced, due to which the consumer will then be forced to upgrade for better services. Another method is also by offering something, such as a metal card which is an attractive offer to the consumer. According to Expert A, the freemium business model will move into the traditional banking sector, without a doubt. The other business model Expert A discusses, is the kickback solution, where the banks will receive kickbacks from the partners, e.g., insurance companies, to give them revenue, since they would not get enough of that from their own products. This brings in diversity through the platform they have been able to build. Expert B states that the PSD 2 directive is going to force the banks to let in other actors with open banking, this will then probably reduce the revenue by maybe even a third, or more. Due to this Expert B speculates that the banks will most likely have to expand or be more specific and aim exactly at something which they then would have to be good at.

When asking if the Neobanks would have to make any changes to their business practices, to then attract more of the traditional banks' customers, and how they would then be able to do so, did both Expert A and Expert B answer yes. The conclusion being that they do not have a choice, but it will remain to be seen, who will survive, since the Neobanks would have to change in order to start making a profit. The Neobanks are currently still making a loss, and according to Figure 9 are all Neobanks making a negative net profit per customer. Most Neobanks are driven by venture capital, instead of them actually generating their own money. Since they will not be able to continue very long without turning a profit, they will have to start venturing into other ways of making money, such as lending. Turning towards loans for example would be smart, since you can earn a lot of money, but have little risk, depending on if you do it the right way, e.g., housing loans. According to both the author and Expert A, have Neobanks been attracting

customers due to the fact that people get interested when something is free, but then the difficult part is turning those customers into paying customers. Expert B also stated that there will probably be more of a natural shift in the customer base for Neobanks, since at the moment they are attracting more of a younger customer base, but this will naturally shift, when this young generation gets older.



Fincog Benchmark On Challenger Banks' Features And Profitability

comparison of challenger banks that are centered around debit- or prepaid cards, October 2019

		Revolut	monzo	monese	N26	bunq	MOGO	LUNAR	NUBANK
		REVOLUT	MONZO	MONESE	N26	BUNQ	MOGO	LUNAR	NUBANK
PROFILE	Founded	Jul-15	Feb-16	Oct-13	Feb-13	Mar-12	Aug-03	Aug-15	May-13
	Legal Status	E-money Institution & Bank	Bank	E-money Institution & Credit Institution	Bank	Bank	Credit Institution, Mortgage Broker, Whitelabel Prepaid Card	Bank	Bank
	Customer Segments	Retail & Business	Retail & Business	Retail & Business	Retail & Business	Retail & Business	Retail	Retail & Business	Retail (& waiting list for Business)
	Number of Customers (M)[1]	7.0	3.1	1.4	3.5	0.035	0.900	0.130	12.0
	Valuation ($B)[2,3]	1.8	2.5	n/a	3.5	n/a	0.093	n/a	10.0
	Total Funding ($M)[3]	336	399	80	683	49	201	53	1,100
	Home Country	UK	UK	UK	Germany	Netherlands	Canada	Denmark	Brazil
	International Presence	EEA, Australia, Canada, Singapore, Switzerland, USA (+ expanding to 24 other countries worldwide)	USA (waiting list)	EEA	EEA, Switzerland, USA, (+ Brazil coming soon)	Fully active in Germany, Austria, Italy, Spain, France, Belgium and Ireland, expanding to rest of Europe	-	Norway, Sweden	Argentina, Mexico (waiting list for both)
KEY FEATURES	Current Account (incl. Debit / Prepaid Card)	✓	✓	✓	✓	✓	✓	✓	✓
	International Transfers	✓	✓	✓	✓	✓	-	-	-
	Credit Card	-	-	-	-	✓	-	-	✓
	Savings Account	✓	✓	✓[6]	✓	-	-	-	-
	Investments	✓	-	-	-	-	✓	-	✓
	Personal Loans	-	✓	-	✓	-	✓	✓	✓
	Residential Mortgages	-	-	-	-	-	✓	-	-
	Business Loans	✓	-	-	-	-	-	-	-
	Insurance	✓	-	✓[4]	✓	✓	-	✓	✓
FEE STRUCTURE	Free Current Account	✓	✓	✓	✓	-	✓	✓	✓
	Premium Accounts	✓	-	✓	✓	✓	-	✓	-
	Lending Rates (%)[4]	12.5% - 25% APR for Business Loans	3.7% - 19.5% APR on Personal Loans, and £0.50 per day for overdrafts (max. £15.50 p/m)	n/a	1.99% - 19% p.a.	n/a	5.9% - 45.9% for Personal Loans, 2.59% - 2.85% for 3-5yr Mortgages	0% - 46.6% for Personal Loans	28% - 80% for Personal Loans, 27%-435% for Credit Cards
	Deposit Rates (%)[4]	0%	up to 1.50 %	up to 0.70%[5]	up to 1.48%	0.27%	n/a	0%	6.27%
KEY FINANCIALS	Total Customer Loans ($M)[3,5]	n/a	19.7	n/a	223.7	-	64.8	n/a	1,565.7
	Total Customer Deposits ($M)[3,5]	n/a	568.0	n/a	453.0	232.3	n/a	n/a	584.6
	Total Income ($M)[3,5]	n/a	11.3	-1.4	1.1	0.7	29.1	-2.6	19.1
	Operating Cost ($M)[3,5]	n/a	-73.6	-14.9	-35.0	-12.9	-32.3	-1.7	-176.2
	Net Profit ($M)[3,5]	-40.3	-58.0	-15.4	-35.3	-12.2	-16.5	-3.9	-24.1
RATIO PER CUSTOMER	Valuation Per Customer ($)	250	799	n/a	1,000	n/a	103	n/a	833
	Loans Per Customer ($)	n/a	6	n/a	64	-	72	n/a	130
	Deposits Per Customer ($)	n/a	183	n/a	129	6,636	n/a	n/a	49
	Income Per Customer ($)	n/a	3.63	-1.02	0.31	19.72	32.38	-19.78	1.59
	Cost Per Customer ($)	n/a	-23.76	-10.62	-10.00	-369.12	-35.90	-12.70	-14.68
	Net Profit Per Customer ($)	-5.76	-18.71	-10.98	-10.07	-349.40	-18.35	-30.28	-2.01

fincog

Notes:
1. Number of customers as per the most recent data available
2. Valuation as per the most recent funding round
3. Financial data converted to USD, based on the following exchange rates: GBP / USD = 1.23 ; EUR / USD = 1.10 ; CAD / USD = 0.75 ; DKK / USD = 0.15 ; BRL / USD = 0.24
4. Pricing of loans and deposits based on the home country
5. Financial data as per the most recent annual financial statements
6. Monese offers a marketplace with partners including insurance providers and has a partnership with Raisin for access to their savings marketplace. The deposit rate refers to the interest rate offered at Raisin

Sources: Company Websites, Annual Reports, Press Search, Fincog Analysis

Figure 9. Fincog Benchmark On Challenger Banks' Features And Profitability.

Next, we considered the changes in EU laws and regulations such as PSD 2, through which Neobanks have been able to enter the market, and if regulations should more include Neobanks for future purposes. Both Expert B and Expert A made the point that you do not make laws for a specific group of companies such as Neobanks, since you make laws for all actors in the same area of business, such as banks in general. Commenting on the PSD 2 directive, Expert A thinks that it will work in favour of Neobanks on a short term, but they cannot obtain longer-term leverage from the integration of a specific customer's all accounts to that one specific bank through the open

banking and API's. This is because the traditional banks have already shown interest towards this opportunity, as well as started the production of such services. The way Neobanks would then instead be able to utilise the PSD 2 and open banking framework, is through for example interest matching, states Expert A. This would mean that the Neobank would also be able to make a good and informed credit assessment through being able to gather more information on the consumer, their spending habits and income streams, through which the credit assessment would reduce some of the risks. The traditional banks would probably stay within lower risk loan such as housing loans.

According to both Expert A and Expert B is the impact of internet of things, on the banking industry still very small, or non-existent. Internet of Things (IoT) will probably be huge someday in the future, but at the moment it is very minimal and on a baby step level. Mobile payments being the first step taken in the area of IoTs, but when looking globally and comparing Europe to for example China, is Europe nowhere near that. A positive impact of something as mobile pay or Swish, is the lower costs it generates for merchants, since they do not have to pay everyone around in the system. Both Expert A and Expert B commented on the current regulations disabling some IoT possibilities, such as having your refrigerator ordering food for you every time you run out of something specific or being able to just tell your Google Home to make a bank transfer to some specific account. Expert B also pointed out the fact that consumers have a need for everything to work frictionlessly, easy, simple and fast, until something unwanted happens to your information, after which you would have wished that the merchant had authentication and extra safety mechanisms.

Further the interview discussions revolved around biggest risks with cryptocurrency from the AML and KYC perspectives. Expert A commented that the biggest risks are of course the exchange websites, which allows the clients to receive money and send money freely, after which, allowing clients to make an exchange to fiat currency though the traditional banking system. The fact that the banks are lacking in a good way of tracking and monitoring the transactions and where they are coming from, is this one big AML risk. The issue stems from places in the world, which do not have as strong regulations, or good financial crime systems, and then people being able to commit fraud in these countries, change the money to a cryptocurrency and move that to a more regulated area. Even though there are good tracking software's being developed and appearing, is the banking industry still way behind in their implementation of them. In conclusion on this point, is the possibility of fraud and crime due to cryptocurrencies the biggest risks regarding these cryptocurrencies according to both Expert A and Expert B.

Lastly the interview discussions revolved around which effects of open banking and the PSD 2 directive has had on the banking industry. Expert A commenting that he was a little surprised that the effect has been very marginal, since he expected it to have a bigger impact. We have not yet seen a big difference in the product offering but he predicts that we will see a boom in banking service providers, since companies will be able to act as a bank, without having to actually be a bank, and run their customer interface and provide the banking services whilst the traditional banks have to do all the work regarding AML, as well as run the infrastructure with the actual costs of running a bank. Expert A then finally comments that he is though sure that the traditional banks are going to be able to act very quickly when they have realized that this is an actual threat and have everything up and running within a year. Expert B also making the point that the PSD 2 is going to impact some banks revenues hard and forcing them to find other ways of earning that money but have a positive impact for the Neobanks.

5 Conclusions

This thesis research question was what are the challenges, risks and opportunities related to the Neobanks. The investigative questions which were supporting the research question were: what new possibilities have Neobanks brought to banking customers, what new risks are associated with Neobanks, and what does the sustainability of the Neobank ecosystem and future challenges on a societal level look like.

The first investigative questions about what new possibilities have Neobanks brough to banking customers, was researched through section in the thesis on the customer experience and especially services provided. The second investigative question, what new risks are associated with Neobanks has been researched in this thesis particularly within the technology and cybercrime sections, as well as separately in the researched information on the Neobanks onboarding process risks, relating to AML risks. The research also revolved slightly around cryptocurrency as well as the internet of things, relating to the investigative question two. The third investigative question on the sustainability of the Neobanks ecosystem and future challenges on a societal level, can be directly linked to the laws and legislations researched. These investigative questions can also be linked to the interview questions relating to risks within the industry, future business model, as well as the need for changes in business practices.

Based on the results received through the conducted research, the author has found detailed answers to all the three facets of the research question related to the Neobanks, as well as the whole banking industry more generally.

5.1 Reliability and Validity of the Study

The potential lack in accuracy is due to the possibility of not finding sufficient and trustworthy enough source materials to be able to get a full picture of the Neobanks business practices. Since the Neobanks are a new phenomenon, there has been very little academic research conducted on them, and no relevant academic studies were found in an exhaustive search. Consequently, most sources included in the thesis are non-academic based, for example, coming from major international consultancy companies. Additionally, understanding the laws and regulations, and an accurate interpretation by the author is another risk factor concerning the accuracy of this thesis.

5.2 Key Outcomes

The author has been able to enhance her knowledge and understanding of the banking industry, and especially the laws and regulations relating to the industry, both domestic and international ones, on an EU level as well as UK level. Intensive personal learning and growth did happen through this project. It was particularly inspiring to interact with the financial experts and learn from their broad perspectives and knowledge base.

5.3 Suggestions for Further Research

In contrast to the pre-internet dominated era, the banking world is currently a fast and an ever-changing industry. The traditional banks will likely have to adapt and change to keep the market shares they currently possess also in the future. Also due to COVID-19 has the need increased for being able to manage your personal banking online-only.

Further studies could revolve around the effects of COVID-19 on the banking services, as the pandemic may have affected the traditional banks to focus even more on the online-only banking methods, and close more branches.

Further studies might also include research on how the Neobanks do survive, will they stay alive in the longer term, or will recessions' affect them, like the last global financial crisis starting in 2008 which caused the Icelandic online banks to go bankrupt.

It is currently uncertain how the market will change, for example will the Neobanks take over traditional bank's roles, and if so, what will be the traditional banks role in the future? Further research should preferably be conducted on the topic at a deeper level, for example, corresponding to a master's degree research paper.

References

Accenture 2019. Be safe: Cybercrime in the financial services industry. URL: https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50. Accessed: 4 February 2021.

Ballard, B. 2018. The unstoppable rise of neobanks. World Finance. URL: https://www.worldfinance.com/banking/the-unstoppable-rise-of-neobanks. Accessed: 4 February 2021.

Bank of England and Financial Services Act 2016.

Abedine, A. Burchardi, K. Buser, M. Golebiowska, A. Kronfellner, B. Lai, C. Mogul, Z. Rhode, W. Vallabhaneni, P. Wagner, J. & Wee, K. 2020. How Banks Can Succeed With Cryptocurrency. URL: https://www.bcg.com/publications/2020/how-banks-can-succeed-with-cryptocurrency. Accessed: 27 March 2021.

Danske Bank 2018. Our approach towards cryptocurrencies. URL: https://danskebank.com/news-and-insights/news-archive/news/2018/23032018. Accessed: 5 September 2020.

Danske Bank 2019. Annual Report. URL: https://danskebank.com/-/media/danske-bank-com/file-cloud/2020/2/annual-report-2019.pdf?rev=ce58f68c871c451ab82c07640edbc51f&hash=091E45286122B94B1F719CEA4F23A799. Accessed: 1 March 2021.

Danske Bank 2020. Sinulle. URL: https://danskebank.fi/sinulle. Accessed: 1 September 2020.

Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC.

Directive 2014/92/EU of the European Parliament and of the Council of 23 July 2014 on the comparability of fees related to payment accounts, payment account switching and access to payment accounts with basic features.

European Bank Authority 2020. Report on Competent Authorities'' Approaches to the Anti-Money Laundering and Countering the Financing of Terrorism Supervision of Banks. URL: https://www.eba.europa.eu/sites/default/documents/files/document_library/News%20and%20Press/Press%20Room/Press%20Releases/2020/EBA%20acts%20to%20improve%20AML/CFT%20supervision%20in%20Europe/Report%20on%20CA%20approaches%20to%20AML%20CFT.pdf. Accessed: 9 April 2021.

European Payments Council 2017. PSD2 EXPLAINED. URL: https://www.europeanpaymentscouncil.eu/sites/default/files/infographic/2018-04/EPC_Infographic_PSD2_April%202018.pdf. Accessed: 4 April 2021.

Eurostat 2020. COVID-19 impact on employment income. URL: https://ec.europa.eu/eurostat/web/products-eurostat-news/-/DDN-20201210-2. Accessed: 15 February 2021.

Exton consulting 2020. NEOBANKS 2021 – SHIFTING FROM GROTH TO PROFITABILITY? URL: https://extonconsulting.com/en/wp-content/uploads/sites/2/2020/11/Inside-Financial-Services-Germany-n5.pdf. Accessed: 6 March 2021.

Finance Derivative 2021. 1 IN 4 MILLENNIALS AND GEN-ZS ARE USING CHALLENGER BANKS WITH MONZO THE MOST POPULAR. URL: https://www.financederivative.com/1-in-4-millennials-and-gen-zs-are-using-challenger-banks-with-monzo-the-most-popular/. Accessed: 6 March 2021.

FIN-FSA 2018. Basic banking services. URL: https://www.finanssivalvonta.fi/en/Consumer-protection/questions-and-answers/banking-services/basic-banking-services/. Accessed: 14 May 2020.

FIN-FSA 2018a. Luottolaitokset. URL: https://www.finanssivalvonta.fi/pankki/luottolaitokset/. Accessed: 17 September 2020.

FIN-FSA 2018b. Maksupalvelun tarjoajia koskeva lainsäädäntö. URL: https://www.finanssivalvonta.fi/pankki/maksupalvelun-tarjoajat/saantely/lainsaadanto/. Accessed: 16 March 2021.

Florian 2021. SEON. How Can NeoBanks Offer Digital Onboarding That's Both Safe And Easy. URL: https://seon.io/resources/how-can-neobanks-offer-a-digital-onboarding-process-thats-both-safe-and-easy/. Accessed: 20 April 2021.

Frankenfield, J. 2020. Online banking. Investopedia. URL: https://www.investopedia.com/terms/o/onlinebanking.asp. Accessed: 14 May 2020.

Ghosh, A. 2016. Smartphone bank N26 is not safe and exposes users to hacking, says researcher. International Business Times. URL: https://www.ibtimes.co.uk/smartphone-bank-n26-not-safe-exposes-users-hacking-says-researcher-1598474. Accessed: 4 February 2021.

2017 No. 692. FINANCIAL SERVICES. The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017.

GOV.UK 2021. Anti-money laundering registration. URL: https://www.gov.uk/anti-money-laundering-registration. Accessed: 4 April 2021.

HCL 2021. WHAT ARE THE DIFFERENT IT TECHNOLOGY RISKS IN FINANCIAL SERVICES? URL: https://www.hcltech.com/technology-qa/what-are-different-it-technology-risks-in-financial-services. Accessed: 4 February 2021.

Houben & Snyers 2018. Cryptocyrrencies and blockchain. URL: https://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf. Accessed: 25 March 2021.

IFA, 2021. Money laundering Regulations 2017. URL: https://www.ifa.org.uk/technical-resources/aml/uk-law-and-guidance. Accessed: 9 April 2021.

ImmuniWeb 2019. State of Application Security at S&P Global World's 100 Largest Banks. URL: https://www.immuniweb.com/blog/SP-100-banks-application-security.html. Accessed: 5 September 2020.

ING, 2018. How do you prefer to pay? URL: https://think.ing.com/uploads/reports/ING_International_Survey_Mobile_Banking_2018_-_ways_to_pay.pdf. Accessed: 18 February 2021.

Insead, J. 2002. The transformation of the European financial system. European Central Bank. URL: https://www.ecb.europa.eu/events/pdf/conferences/dermine_comp.pdf. Accessed: 16 March 2021.

Kagan, J. 2020. Financial Technology – Fintech. Investopedia. URL: https://www.investopedia.com/terms/f/fintech.asp. Accessed: 6 February 2021.

Laki pankki ja maksutilien valvontajärjestelmästä 571/2019.

Laki rahanpesun ja terrorismin rahoittamisen estämisestä 28.6.2017/444.

Laki rahanpesun selvittelykeskuksesta 28.6.2017/445.

Laki talletuspankkien toiminnasta 1268/1990.

The law society, 25 Feb 2020. Quick guide to the Money Laundering Regulations 2017. URL: https://www.lawsociety.org.uk/en/topics/anti-money-laundering/quick-guide-to-the-mlrs. Accessed: 15 April 2021.

LexisNexis 2021. What is Know Your Customer (KYC)? URL: https://bis.lexisnexis.co.uk/due-diligence-and-compliance/glossary/kyc. Accessed: 9 April 2021.

Linklaters 2021. EU opens door for cryptocurrency exchanges to apply AML rules. https://www.linklaters.com/en/insights/blogs/fintechlinks/2018/june/eu-opens-door-for-cryptocurrency-exchanges-to-apply-aml-rules. Accessed: 25 March 2021.

Maksulaitoslaki 30.4.2010/297.

Maksupalvelulaki 30.4.2010/290.

Morgan J, 2014. A simple explanation of the internet of things. Forbes. URL: https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/?sh=546204091d09 Accessed: 16 March 2021.

Muldrew, E. 2020. The rise of Neobanks Disrupting the banking industry. URL: https://edwardmuldrew.medium.com/the-rise-of-neobanks-disrupting-the-banking-industry-5976e95b5d14. Accessed: 4 February 2021.

N26 2019. N26 now has over 1 million customers in France! URL: https://n26.com/en-eu/blog/n26-now-has-over-1-million-customers-in-france. Accessed: 12 February 2021.

N26 2020. Find a plan for you. URL: https://n26.com/en-eu/plans. Accessed: 29.9.2020.

N26 2020a. What does N26 do with my tax information? URL: https://support.n26.com/en-eu/account-and-personal-details/taxes/what-does-n26-do-with-my-tax-information?gh_jid=958865. Accessed: 28 August 2020.

Nordea 2020. Henkilöasiakkaat. URL: https://www.nordea.fi. Accessed 1 September 2020.

Nordea 2020a. Tervetuloa Nordeaan. URL: https://www.nordea.fi/henkiloasiakkaat/tule-asiakkaaksi/tule-asiakkaaksi-verkossa.html. Accessed 12.8.2020.

OP 2020. Know Your Customer. URL: https://www.op.fi/know-your-customer. Accessed: 17 September 2020.

Orlando, S. 2020. The differences between traditional and online banking. Expatica. URL: https://www.expatica.com/be/finance/banking/the-differences-between-traditional-and-online-banking-1299954/. Accessed: 14 May 2020.

Pritchard, J. 2019. What Is a Neobank (and should You Try One)?. URL: https://www.thebalance.com/what-is-a-neobank-and-should-you-try-one-4186468. Accessed: 16 April 2020.

PWC 2021. Making sense of bitcoin, cryptocurrency and blockchain. URL: https://www.pwc.com/us/en/industries/financial-services/fintech/bitcoin-blockchain-cryptocurrency.html. Accessed: 25 March 2021.

Revolut 2020. Cryptocurrency. URL: https://www.revolut.com/legal/cryptocurrency-terms. Accessed: 15 February 2021.

Revolut 2020a. Our Pricing Plans. URL: https://www.revolut.com/en-FI/our-pricing-plans. Accessed: 29 September 2020.

Revolut 2021. Is my money safe? URL: https://www.revolut.com/en-PL/help/profile-plan/security-personal-data/is-my-money-safe. Accessed: 7 March 2021.

Revolut 2021a. Revolut Personal terms. URL: https://www.revolut.com/en-FI/legal/terms. Accessed: 20 April 2021.

Revolut 2021b. Cryptocurrency. URL: https://www.revolut.com/en-FI/legal/cryptocurrency-terms. Accessed: 20 April 2021.

S-Pankki 2020. S-Pankki. URL: https://www.s-pankki.fi. Accessed: 1 September 2020.

Shevlin, https://www.forbes.com/sites/ronshevlin/2020/02/03/the-5-hottest-technologies-in-banking-for-2020/. Accessed: 18 February 2021.

Slaughter and May 2019. Banking Regulation in the United Kingdom. URL: https://www.lexology.com/library/detail.aspx?g=4e55a6bc-5f01-4abd-b242-d6e0bdf3f405. Accessed: 9 April 2021

Statista 2020. Forecasted number of downloads worldwide of European app-only banks from January 2015 to December 2021, by bank. URL: https://www.statista.com/statistics/1126745/monthly-number-neobank-app-downloads-worldwide-forecast/. Accessed: 4 February 2021.

Stevenson, M. 24.11.2020. Banks vs Neobanks: What is a Neobank? URL: https://mikemba.medium.com/banks-vs-neobanks-what-is-a-neobank-34cb05778945. Accessed: 6 March 2021.

Trustly 2021. Open Banking Around the World. https://www.trustly.net/open-banking/open-banking-around-the-world. Accessed: 16 March 2021.

Appendices

Appendix 1. Interview Questions.

1. Will the traditional banks have to change their business practices fast and drastically to keep up with the rising Neobanks?
   a. If not, why?
   b. If yes, how should they change their business practices?

2. What will be the leading business model in the banking sector in the near future, within a 5-year time frame?

3. Will Neobanks change their business practices to attract more of the traditional bank's customers?
   a. If yes, how would they do this?
   b. If not, why do you think they won't?

4. Changes in EU Laws and regulations, such as PSD and PSD 2 have opened up the possibility of Neobanks entering the market, but should EU specify directives and regulations to more include Neobanks for future purposes?

5. What are some positive and negative impacts that the internet of things has had on the banking industry?

6. What are the biggest risks with cryptocurrency from the AML and KYC perspective in your opinion?

7. What type of positive and negative effects has open banking and the PSD 2 directive had on the banking industry?

Appendix 2. N26 Basic pre-contractual information, 1 March 2019.

Basic pre-contractual information

For contracts negotiated away from business premises and distance contracts on the rendering of financial services and payment services framework contract, as well as for contracts in electronic commerce.

(Version 1.3, Date: 02.09.2019)

Name and address of N26 Bank GmbH

N26 Bank GmbH
Klosterstrasse 62
10179 Berlin

Telephone: +49 (0) 30 364 286 880
Email: support@n26.com

(hereinafter referred to as "N26")

Legal authorised representative of N26 Bank GmbH

Legal authorised representatives of N26 are: Markus Gunter, Richard Groeneveld.

Main activity of N26 Bank GmbH

The main activity of N26 is the operation of various types of banking businesses and other associated businesses.

Responsible regulatory authority

The regulatory authority responsible for N26 is the (German) Bundesanstalt für Finanzdienstleistungsaufsicht i.e. Federal Financial Supervisory Authority (Graurheindorfer Straße 108, 53117 Bonn und Marie-Curie-Str. 24-28, 60439 Frankfurt am Main, www.bafin.de). N26 is registered under the number 145827 in the company database in the Federal Institute for Financial Services Supervision.

Deposit protection fund

N26 is affiliated with the deposit protection fund of the Entschädigungseinrichtung deutscher Banken GmbH (German Banks Compensation Scheme). The deposit protection fund secures all liabilities which are to be disclosed in the balance sheet position, "liabilities towards Customers". Demand, term and savings deposits are included.

Entry (of the head office) in the trade register

District court Berlin (Charlottenburg) HRB 170602

N26

Value added tax identification number

DE 30/595/7096

Minimum term of the contract

There exists no minimum term of the contract for a N26 current account.

Contractual termination rights

You can cancel your N26 current account without notice as set out in §18 of our T&Cs (Basic Rules Governing the Relationship Between the Customer and the Bank). We can cancel the current account with notice of two months as set out in §19 of our T&Cs (Basic Rules Governing the Relationship Between the Customer and the Bank).

Prices

You can find the applicable prices in our current pricelist.

Applicable law/court of jurisdiction

German law is applicable for the business relationship between you and N26. N26 is also subject to the law of the Federal Republic of Germany for the pre-contractual relation. There is no contractual clause stipulating jurisdiction.

Information and language of contract/text of the contract

The governing language for this contractual relationship and the communication between you and N26 during the period of the contract is German. The terms and conditions are available in the German. The Customer has the right to demand the communication of these contract conditions in text form at any point in time during the contract period.

Option of legal remedy/extrajudicial settlement of disputes

- Due to disputes arising from the application of the Payment Services Supervision Act (Zahlungsdiensteaufsichtsgesetzes- ZAG), the provisions of the German Civil Code (Bürgerliches Gesetzbuch – BGB) concerning distance contracts for the rendering of financial services, the regulations for payment services (§§ 675c – 676c BGB) and for consumer loans (§§ 491 to 509 BGB), or of article 248 of the Introductory Act to the BGB, you can call upon the arbitration body that is established at the German Federal Bank (Deutsche Bundesbank), and/or lodge a complaint with the German Federal Financial Supervisory Authority (Bundesanstalt für Finanzdienstleistungsaufsicht) without prejudice to its right to bring the matter before the court.
- Furthermore the European commission has set up an European online dispute resolution platform (ODR Platform) for businesses in connection with online contracts for services to be settled by customers out of court. The ODR Platform can be accessed under the following link: http://ec.europa.eu/consumers/odr/

N26

Service proviso

There is no service proviso, unless explicitly agreed.

Technical steps for the conclusion of the contract

Requirements and supported smartphones

In order to use your N26 account, you need an associated smartphone. Although you can use some features of your account without an associated telephone, for security reasons, essential features only function on the telephone that has been specifically associated with your account. Since your smartphone is used as a personal authentication device, only one phone at a time may be connected to your account. For security reasons, the associated smartphone may also be required to verify logins from other devices. Please note that your device is meeting the respective minimum requirements for the operating system (iOS / Android) and the N26 app. Currently supported versions and further information can be found in the N26 Support Center. Due to security reasons we are forced to discontinue our service for any out-dated versions of the respective operating system and out-dated versions of the N26 app version. We will notify you eight weeks before we stop supporting a version of the respective operating system in case this disables you to use the N26 App and invite you to update your software during that period of time.

In addition to essential features, such as viewing your transactions and settings, the following features are only available on your associated smartphone:

- Successfully completing registration with N26
- Confirming transfers and standing orders
- Confirming MoneyBeams and CASH26 transactions
- Applying an overdraft credit
- Associating a smartphone

If no smartphone is currently associated with your account, simply open the N26 app on your phone. The N26 app, depending on the smartphone you use, is available through distribution platforms operated by third-parties ("app-stores"). Your association requires prior registration in the corresponding app-store.

After installing the app, you will be automatically taken through all the necessary steps to associate your smartphone:

- Confirm your telephone number
- Receive a four-digit code via SMS
- Enter the code in the app to complete the association

If the phone number displayed during the association is not correct, or if you do not receive the SMS association code despite the phone number being correct, please contact Customer Service.

Opening of your N26 Bank account

To start the application, create a user account in the N26 app on your smartphone or the N26 web-app. Completing the registration with N26 requires agreement to our general terms and conditions, as well as your consent to our conditions for a credit check. Then, confirm your email address. We will send an email to the

email address that you specified during registration containing a link. Now, you can confirm your identity directly in the N26 app. Once you have confirmed your identity, you must associate your smartphone with your account.

Setting a transfer PIN

You can set the transfer code for your N26 account yourself. This has the advantage that you may pick a PIN that you can easily remember. You will be prompted to enter the transfer PIN after you have associated your smartphone with your account for the first time.

Your transfer PIN is a four-digit combination that you need for the execution of any transfer of funds or MoneyBeams, and for the establishment of standing orders and CASH26 barcodes. For security reasons, some number combinations cannot be used:

- PINs containing parts of your date of birth
- PINs containing parts of your address, such as your postal code
- Repetitions of numbers, such as 1111
- Number series, such as 1234

If your desire PIN is not accepted, please try another combination. Note, as well, that, although not all combinations are accepted, you can always assign a transfer PIN that is identical to the PIN for your card.

If you have incorrectly entered your transfer PIN six times in a row, the PIN is locked for security reasons. Please change the transfer PIN according to the instructions above in order to unlock it again.

Possibility for correction of entry errors

You have the ability to detect and correct entry errors. For this purpose, you will receive confirmation displays, in which a summary of your information will be described and the opportunity will be given to you to either correct the information or to open your account with the appropriate information and product variants.

Retrieval and storage possibility for contractual conditions

You have the ability to retrieve and view all the contractual provisions from your contract with N26 on N26's website.

Codes of conduct

N26 Bank observes statutory regulations; there exist no specialised codes of conduct.

Appendix 3. N26 Depositor information, 26 October 2016.

N26

Depositor information

With the following "Depositor Information Sheet", we, N26 Bank GmbH, wish to inform you – pursuant to Section 23a (1) sentence 3 of the German Banking Act (Kreditwesengesetz, KWG) – about the statutory Deposit Guarantee Scheme.

(Version 1.1., Date: 26.10.2016)

Deposits at N26 Bank GmbH, Klosterstraße 62, 10179 Berlin are protected by:
German Banks Compensation Scheme [1]

Limit of protection
EUR 100,000 per depositor per credit institution [2]

If you have more deposits at the same credit institution
All your deposits at the same credit institution are 'aggregated' and the total is subject to the limit of EUR 100,000 [2]

If you have a joint account with other person(s)
The limit of EUR 100,000 applies to each depositor separately [3]

Reimbursement period in case of credit institution's failure
Within 7 working days from 1 June 2016 [4]

Currency of reimbursement
Euro

Contact

Entschädigungseinrichtung deutscher Banken GmbH

Burgstraße 28, 10178 Berlin, GERMANY

Postal address:
Postfach 11 04 48
10834 Berlin
GERMANY

Telephone:
+49 (0)30 59 00 11 960

Email:
info@edb-banken.de

More information
www.edb-banken.de [5]

N26

(1) Your deposit is covered by a statutory Deposit Guarantee Scheme and a contractual Deposit Guarantee Scheme. If insolvency of your credit institution should occur, your deposits would in any case be repaid up to EUR 100,000.

(2) If a deposit is unavailable because a credit institution is unable to meet its financial obligations, depositors are repaid by a Deposit Guarantee Scheme. This repayment covers at maximum EUR 100,000 per credit institution. This means that all deposits at the same credit institution are added up in order to determine the coverage level. If, for instance, a depositor holds a savings account with EUR 90,000 and a current account with EUR 20,000, he or she will only be repaid EUR 100,000.

(3) In case of joint accounts, the limit of EUR 100,000 applies to each depositor. Deposits in an account to which two or more persons are entitled as members of a business partnership, association or grouping of a similar nature, without legal personality, are aggregated and treated as if made by a single depositor for the purpose of calculating the limit of EUR 100,000. In the cases listed in Section 8 (2) to (4) of the German Deposit Guarantee Act (Einlagensicherungsgesetz) deposits are protected above EUR 100,,000. More information can be obtained from the website of Entschädigungseinrichtung deutscher Banken GmbH at www.edb-banken.de.

(4) If you have not been repaid within these deadlines, you should contact the Deposit Guarantee Scheme since the time to claim reimbursement may be barred after a certain time limit. More information can be obtained from the website of Entschädigungseinrichtung deutscher Banken GmbH at www.edb-banken.de.

(5) In general, all retail depositors and businesses are covered by Deposit Guarantee Schemes. Exceptions for certain deposits are stated on the website of the responsible Deposit Guarantee Scheme. Your credit institution will also inform you on request whether certain products are covered or not. If deposits are covered, the credit institution shall also confirm this on the statement of account.

Appendix 4. N26 General terms and conditions "N26 current account", 16 July 2019.

N26

General terms and conditions „N26 current account"

(Version 1.5., Date: 16.07.2019)

1. Scope of application

1.1

These General Terms and Conditions ("AGB") are applicable for all the banking services of N26 Bank GmbH ("N26", "we"), which you ("End user", "You") can use via the application of the mobile App named "N26" ("App") or via the online interface provided by N26 GmbH that can be accessed under https://my.n26.com ("Online Interface"). Additionally, the following conditions are also applicable, insofar as they do not contradict the provisions of these General Terms and Conditions.

- Basic pre-contractual information
- Depositor information
- General Business Conditions - Basic Rules Governing the Relationship Between the Customer and the Bank
- Terms and Conditions for Credit Transfers
- Terms and Conditions for eBanking
- General Terms and Conditions for Payments by Direct Debit under the SEPA Core Direct Debit Scheme
- Terms and Conditions for Private and Business MasterCard Debit Cards
- Special Conditions for Digital Account Statements
- Price list

1.2

The supplementary terms of use, which you can view below are applicable for the use of the App and the Online Interface ("End Customer interfaces").

2. Object of service

2.1

The object of service is the management of a current account and the issue of the N26 MasterCard ("Account"). You can operate and manage the account via the end Customer interfaces. The prerequisite is a smartphone that is linked to the account, which fulfils the respective minimum requirements for the operating system (IOS/Android) and our N26 app version. (Currently supported versions and further information can be found in the N26 Support Center). Due to security reasons we are forced to discontinue our service for any out-dated versions of the respective operating system and out-dated versions of the N26 app version. We will notify you eight weeks before we stop supporting an version of the respective operating system and invite you to update your software during that period of time.

The current account contract includes the following services in detail:

- Account Management

- Payments at ATM's
- Transfers
- Standing Orders/Debit Orders
- Debit Notes (direct debits are excluded in the Customer order)
- MasterCard

2.2

The account is used for the processing of payment transactions and the processing of card revenues from the linked MasterCard.

2.3

The credit balance on the account is payable on a daily basis. The account is managed on a current account ("open account") basis. The account is managed as credit account. Please note the overdraft facility on the basis of staggered synchronisation processes (Clause 11). Furthermore, an overdraft credit contract subject to your credit rating can also be concluded with us separately.

2.4

The transaction limit stipulated for the cash service is applicable within your credit limit that you may access via the N26 Support Center As a rule, changes to the applicable limit will be agreed separately with you.

2.5

You will not receive any interest on the account balance.

2.6

The N26 Invest feature is described under Clause 7.4.

2.7

The N26 You membership is described under Clause 7.5.

2.8

The N26 Business feature is described under Clause 7.6.

3. Account opening

3.1

You can open an account, on the condition you are at least 18 years old, have a smartphone, on which the Apps mentioned under Clause 3.2 are installed and can be used and you reside in one of the countries mentioned via in N26 Support Center and you have not yet opened an account with us. The opening of multiple accounts is not permitted. The opening of an account is only permissible for a natural person. If any identifiable business turnover is transacted via the private current account – with the exception of the regulation in Clause 7.7 - we have the right to terminate the account under compliance of an appropriate notice period.

N26

3.2

If you would like to open an account via the App, you must first download it. (Please find information on this in the N26 Support Center)

3.3

To open an account via online interface, please visit the website: https://www.n26.com.

3.4

After opening the installed App or the online interface, a registration process begins, under which you can apply electronically for the opening of an account.

3.5

By submitting an electronic account opening application to N26, you are submitting a binding offer for the conclusion of a contract for the provision of an account with the functions described under Clause 2 of these General Terms and Conditions.

4. Identity verification, conclusion of contract

4.1

We are legally obliged to verify your identity prior to the opening of an account. You have the following options:

Identification via PostIdent process by the employees of Deutsche Post AG ("Deutsche Post") (please find more information on this in the N26 Support Center)

Video chat based identification by the employees of IDnow GmbH, Fuerstenstrassse 15, 80333 Munich ("IDnow"), (please find more information on this in the N26 Support Center)

Personal identification checks may be carried out by our employees in exceptional cases.

4.2

A contract for the provision of an account with the functions described under Clause 2 of these General Terms and Conditions is concluded when we confirm that we have set up an account for you ("Contract"), either via SMS, e-mail or in any other mode of direct communication.

---

5. Revocation policy

Revocation right

You can revoke your contract declaration within 14 days without justification in text form (e.g. e-mail). The notice period begins upon receipt of this instruction on a durable data carrier, but not prior to contract conclusion and not before the fulfilment of our information duties as per Article 246b § 2 (1) in conjunction with § 1 (1) Number 7 to 12, 15 and 19 as well as Article 248 § 4 (1) EGBGB [Introductory Act to the German Civil Code]. A timely dispatch of the revocation is adequate for safeguarding the revocation deadline. The revocation must be sent to:

N26

N26 Bank GmbH
Klosterstrasse 62
10179 Berlin

E-Mail:
terms@n26.com

Revocation consequences

In the event of effective revocation, the services received by both parties must be returned and, if applicable, benefits drawn from the services (e.g. interests) must be surrendered. If you exceed the permitted overdraft amount, we may demand neither costs nor interest beyond the repayment of the amount of the excess if we have not properly informed you of the conditions and the consequences of exceeding the overdraft (e.g. applicable borrowing rate, costs). You are committed to pay compensation for the services provided until the point of time of revocation, if this legal consequence was already conveyed to you prior to the submission of your contract declaration and you have explicitly agreed that we shall begin with the execution of return service prior to the end of revocation deadline. If there exists an obligation for the payment of compensation, then this can lead to the situation that you are still bound to fulfil the contractual payment obligations for the time period up to the revocation. Your right of revocation shall expire prematurely if the contract has been fulfilled completely from both parties upon your explicit request, before you have exercised your right of revocation. Obligations to reimburse payments must be fulfilled within 30 days. The term begins with the dispatch of your revocation declaration on your part, whereas on our part, it starts at the point of time in which we receive the documents.

Special instructions

After the revocation of this contract, you are no longer bound by any other contract that is linked to this contract, on the condition the linked contract concerns a service provided by us or by any third party based on the agreement between us and the third party.

END OF REVOCATION INSTRUCTION

---

6. Language of contract and communication

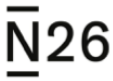
6.1

English is the language of the contract and communication.

6.2

Information and declarations, which concern your contractual relationship with us on the basis of these General Terms and Conditions or which are related to the same, should be sent to the following address, unless specified otherwise in these General Terms and Conditions or requested otherwise by N26:

Email:
Support@n26.com



Phone:
+49 (0) 30 364 286 880

Address:
N26 Bank GmbH, Klosterstrasse 62, 10179 Berlin

6.3

Please always use your registered Email address for submitting legally binding declarations with N26.

7. Use of account

We identify you as an account holder authorised for making payments with the help of payment authentication instruments.

7.1 Linked smartphone as authentication instrument

The combination of a smartphone that is initially linked to your account and has a personalised safety feature is used as an authentication instrument. You can only release the payment transactions with this combination. You will receive detailed information about the linking of smartphones in the N26 Support Center.

7.2 Personalised security features

A unique combination of e-mail address and password, which you can set up yourself while opening an account and with which you can log on to the end user interfaces and set a PIN that enables you to release payment transactions upon request ("Personalised security feature") operates as personalised security feature. You can set this PIN yourself by following the process described in the N26 Support Center.

7.3 Credit transfers and direct debits

Credit transfer orders and direct debits can be issued exclusively in Euro to SEPA accounts. The general terms and conditions for credit transfers and payments by direct debit under the SEPA core direct debit scheme apply.

7.4 N26 Invest

The N26 Invest feature enables you to instruct N26 via the N26 App with the brokerage of shares (execution only) in investment funds in line with § 1 Paragraph 2 KAGB of the portfolio structures ("Modellportfolios") predefined by vaamo Finanz AG. In order to do this, you must submit the brokerage order to N26 and open a securities account with the FIL Fondsbank GmbH. You can find further information in the Terms and Conditions of N26 Bank GmbH for the Product "N26 Invest"

7.5 N26 You

The purpose of N26 You is the provision of special benefits to the Customer in the form of an N26 premium account "N26 You." The contractual services of the N26 Bank GmbH ("N26") specifically include (hereafter together known as the "N26 offer"): 1) the provision of a group insurance policy by N26 together with AWP P&C S.A. – Netherlands subsidiary, acting as Allianz Global Assistance Europe and is a member of the Allianz Group ("Insurer") and 2) the provision of a "N26 You" MasterCard. You can find further information in the Terms and Conditions of N26 Bank GmbH for the premium account "N26 You".

N26

7.6 N26 Business

The purpose of N26 Business is the provision of a Business-MasterCard-debit card, which you can opt to use solely for business purposes. An N26 Business-MasterCard-debit card may only be applied for and used by self-employed natural persons (e.g. freelancers and the self-employed). Use of the Business-MasterCard-debit card is permitted solely for business expenses. Payments made with the card will be debited directly from your N26 account, which, when used in conjunction with the N26 Business-MasterCard-debit card, must also be used predominantly for business purposes.

N26 reserves the right to enquire at any time about the nature of the business use of the N26 Business card and account, as well as about your profession and industry. Independent goods traders are excluded from N26 Business.

7.7 Top Up Feature by Stripe

The Stripe Top Up Feature ("Top Up Feature") is a service provided by our partner Stripe Payments Europe Ltd. ("Stripe"), The One Building, 1 Grand Canal Street Lower, Dublin 2, Ireland. The Top Up Feature provides an easy method for new customers to add funds to their accounts instantly. For this purpose personal data are transmitted to Stripe. You can find further information in our Privacy Policy. The Top Up Feature is provided to eligible customers and is entirely voluntary and free of charge.

7.8 Automatic Billing Program by Mastercard

The Automatic Billing Updater ("ABU") is a service provided by our partner Mastercard Europe S.A., 198/A Chaussée de Tervuren, 1410 Waterloo, Belgium ("Mastercard S.A."), which automatically updates information concerning your Mastercard to third party services you use and to which you subscribed with your Mastercard. By doing this ABU allows you to forgo an update of your account data to third parties by yourself. Thereby ABU aims to reduce preventable card-not-present declines by changes of stored payment account information. For this purpose your personal data are transmitted to Mastercard S.A. You can find further information in our Privacy Policy. The service is free of charge.

8. Non-disclosure of personalised security features; secure storage of authentication instrument

You must maintain secrecy concerning your personalised security features and safely store your authentication instrument. Personalised security features and authentication instrument must be protected from access by a third party.

9. Costs and payment

Remunerations for our services and any expenses to be reimbursed by you are available in our price list, which you can be retrieved via the N26 website. Insofar as the remunerations become due, we calculate these on a quarterly basis and debit them from your account at the end of every quarter, insofar as not otherwise disclosed or stated in the price list.

With respect to overdrafts from your account balance, we calculate the interest on the amount that has been overdrawn as per the stipulation of Clause 11.23, unless a separate overdraft credit agreement has been agreed between you and us.

N26

10. Costs for mobile radio and data transfer

You may incur additional costs for the data transfer depending upon the tariff agreed with your telecommunication provider. These costs must be borne by you and will be invoiced to you by the telecommunication provider.

11. Overdraft of the account and consequences

11.1 Account balance

Payment transactions are permitted only in the scope of the credit balance available in the account. Payment transactions initiated by you that exceed the credit balance available in the account canwill be rejected.

11.2 Interest for account overdraft

If you overdraw your account balance, we shall calculate the interest on the overdrawn amount ("Account overdraft interest"). Unless a separate overdraft credit contract has been concluded with us, the current rate of interest from the overdraft credit agreement is applicable for all overdrafts of your account up to the amount of overdraft facility granted. If no overdraft credit contract has been concluded, we have agreed upon a variable borrowing rate ("account overdraft borrowing rate") for the overdrawn amount equal to 8.9 percentage points above the respectively applicable interest rate for main refinancing companies of the European Central Bank (hereinafter mentioned as "Reference interest rate"). No additional processing fee is charged.

The changes to the account overdraft interest rate depend upon the development of the reference interest rate. This reference interest rate is determined by the council of the European Central Bank and is published in its official interest rate statistics. The council of the European Central Bank presently systematically advises every 6 weeks as to whether the reference interest rate must be adjusted. The initial reference interest rate for the first change of the account overdraft interest rate is the reference interest rate, which was applicable on 1st November 2015 (0:00 hours). This rate is compared with the recently published reference interest rate.

If the recently published reference interest rate has increased by more than 0.25 percentage points as against the initial reference interest rate, then the change of the account overdraft interest rate is triggered and the account overdraft interest rate is increased by the difference. If the recently published reference interest rate is reduced by more than 0.25 percentage points as against the initial reference interest rate, the account overdraft interest rate is reduced by the difference. The change of the account overdraft interest rate becomes effective on the first calendar day of the next month following the publication of the reference interest rate that triggered the change of the account overdraft interest rate.

This likewise applies to further changes of the account overdraft interest rate, with the stipulation that the reference interest rate which was the basis of the last change of the account overdraft interest rate is used as initial reference interest rate.

The bank will inform the Customers at regular intervals regarding the adjusted account overdraft interest rate as well as the due date of the interest payments – if any – on the condition that the latter changes. You will be informed of any adjustments to the account overdraft interest rate.

Factors such as variations in the default risk of the Customer, bank ratings as well as the in-house cost calculation are considered in the adjustment of the account overdraft interest rate.

The interests are subsequently payable at the end of calendar quarter and are charged against the account.

N26

12. Disclosure and notification obligations

12.1

You are obliged to correctly notify us regarding your personal data, in particular your name, address, date of birth, phone number and email address and provide prompt information to us about any changes to this end.

12.2

Immediately inform us regarding a loss or theft of your authentication instrument, your personalised safety features or a misuse or unauthorised use of the same. You can find the relevant contact information in the N26 Support Center on our website.

13. BLOCKING OF THE ACCOUNT AND THE CARD

13.1 Blocking of the account

If we have the reasonable suspicion that any unauthorised use of your account has occurred, we are permitted to block or limit its access. We will inform you promptly via e-mail, SMS or message in the App. Similarly, we will also block your account if you inform us about similar activities. We shall remove the block or the limitation if the reasons for blocking no longer exist.

13.2 Blocking of the card

You have the option to independently block and unblock your card in the end user interfaces. You can report your card as stolen, which will initiate a permanent deactivation of your card and a new card will be sent to you. You also have the option of calling our Customer support and request one of our employees to block your card upon successful authentication.

14. Data protection and bank secrecy

The registration, processing and utilisation of your personal data is conducted under strict maintenance of the applicable legal data protection regulations and simultaneous protection of bank secrecy. You will find further details regarding these regulations in the N26 data privacy policy.

15. Changes to this general terms and conditions (“AGB”)

Information concerning any changes to these General Terms and Conditions and the special conditions will be sent to you by e-mail or by message to your inbox in the App and the Online Interface (Messages from N26) at least two months prior to the proposed time of their date of effectiveness. Your consent shall be deemed as provided if you have not indicated your rejection before the proposed time of the effectiveness of the changes. We will make a specific reference to this de facto acceptance in our offer. If you do not agree with the changes, you can terminate the contract until the point of time the changes take effect without any prior notice. We will make a specific reference to this right to termination in our offer.

16. Applicable law

German law is applicable for the business relation between you and N26.

N26

Supplementary provisions for users of the mobile app “n26” or the online interface that can be reached through https://my.n26.com

1. Preamble

These provisions (“Supplementary Provisions”) apply to the mobile application known as “N26” (the “App”) or the online interface that can be reached through my.n26.com (the “Online Interface”) in addition to the respective applicable conditions of use.

The App and the Online Interface primarily serve to administer your N26 current account, which makes it possible to process transactions using a payment card (the “Card”) licensed by MasterCard Inc. (“MasterCard”). In addition, we use the App and the Online Interface to market our own services and products, and will continually build up this product range in cooperation with further partners.

2. Object of regulation

2.1

These Supplementary Provisions apply to the services and products offered by N26. Furthermore, we would like to inform you about what personal data we collect, process and use.

2.2

Our contract with you comes into existence when we make it possible for you to log in to the App and the Online Interface (acceptance) according to the required data you give when registering (offer). Upon activation by us, a contract between us and you comes into existence on the basis of these Supplementary Provisions. Before giving your offer, you have the opportunity, using the Back button on your browser or smartphone/tablet, as well as using control elements in the App or on the website, to change the data entered, or to completely abort the registration. Your contract with us will be concluded in German. You have the opportunity to call up the contractual provisions, inclusive of these Supplementary Provisions, when concluding the contract, and to store them in reproducible form. No separate storage of the contract text will be done by us.

3. Functionality

3.1

The App and the Online Interface serve for administration of the current account offered by us as well as for the rendering of any other services agreed to with you. The App and the Online Interface are 99% available. Availability indicates, with reference to the term of one (1) contractual year, the relation of the timeframe in which you were able to use the software through an existing Internet connection (plus the timeframe for which access on the basis of planned maintenance works or disturbances was not possible, which lay beyond the influence of N26, such as disturbances in the Internet or disturbances in an app store), in relation to the length of the total contractual year.

3.2

The App as well as the Online Interface is protected by the intellectual property laws, such as copyright law and trademark law. These rights in relation to you are exclusively reserved to us.

3.3

We grant you, exclusively to fulfil the purpose of our contractual relationship with you, the limited, non-exclusive, non-transferable and sub-licensable right, restricted to the period of your contractual relationship with us, to use the App and the Online Interface in accordance with the provisions. The right of use expires upon expiration of the term of the contract.

3.4

The End User is not entitled to (i) rent, lease, lend, reproduce, resell or distribute the App or the Online Interface, or access to them; (ii) use the App or the Online Interface for the development of other services; (iii) activate or use the functionalities of the App or the Online Interface for which no rights of use have been granted to him or her; (iv) assign the usage rights to the App or the Online Interface to third parties, or grant third parties access to the App or the Online Interface; (v) alter, translate, reproduce, or decompile the source code of the App or of the Online Interface, or investigate the functions thereof, outside of what may be legally mandatory in accordance with § 69d or § 69e UrhG (Urheberrechtsgesetz [Copyright Law]); and (vi) remove, conceal or alter legal information, in particular concerning industrial property rights or copyrights of N26.

4. Duties of the user

When using the App or the Online Interface, you are not allowed to perform any illegal actions or breach any applicable laws, in particular not to do the following: infringe industrial property rights, copyrights or intellectual rights of third parties; in your usage behaviour, make defamatory, racist or offensive statements, or undertake such actions; transmit contents which contain viruses, Trojan horses, spyware, adware, malware or other damaging or harmful programmes; distribute unwanted advertising (spam) or any other form of nuisance.

5. Compensation

Compensation for our products and services can be found on the price list, which you can be retrieved yia the N26 website. Provided nothing else is specified, no compensation will be due for the use of the App and the Online Interface.

6. Data protection

6.1 Responsible authority

The responsible authority for the processing of your personal data in connection with the App and the Online Interface and the usages described in Clause 1 above, as well as in connection with any further products and/or services is N26 (for contact data, see Clause 1 above).

6.2 Collection, processing and use of your personal data

We collect, process and use your personal data in harmony with the applicable statutory provisions. All of the personal data collected, processed, and used under our responsibility are stored exclusively for the purpose of fulfilling our contractual relationship with you, and not longer than is required for this purpose.

N26

6.3 Purchase of the App

The App is dependent on the smartphone used by you which is obtainable over third-party sales platforms ("app stores"). Your purchase presupposes a prior registration in the app store concerned. We have no influence on the collection, processing and use of personal data by the relevant app store operator. These are the only responsible authorities in this regard.

6.4 Handling and review of your data; right to information; questions on data protection

At any time, you can view your personal data in the App or in the Online Interface. You can also subsequently change your own password. In order to modify or change further personal data, please get in touch with our Customer Support department: support@n26.com.

Further, you can at any time demand information about the personal data stored which relates to you personally, as well as its origin and recipients and the purpose for which it is being stored. You can reach us using the aforementioned contact data. Questions, suggestions and notes on data protection can also be directed to the contact data mentioned there.

6.5

Otherwise, for the collection, use and processing of personal data, the N26 data privacy policy applies.

7. Consent to the obtainment of notifications and revocation of your consent; Newsletter

7.1

If when installing the App or at a later point in time, you have set up the App or the Online Interface to have news sent to you, you can revoke such approval at any time. You can exercise your right of revocation through a corresponding alteration of the news settings on the App or the Online Interface.

7.2

We send our newsletter with information about products and services from N26 to all end users who have given their approval to receive it, or for whom the preconditions of § 7 Para. 3 UWG (Gesetz gegen den unlauteren Wettbewerb [Law against Unfair Competition]) exist. You can unsubscribe from our newsletter using the link provided for this purpose at the end of any newsletter.

8. Consent to credit assessment from SCHUFA HOLDING AG

You hereby consent to N26 Bank GmbH transmitting data about your application, conclusion and termination of this account to SCHUFA Holding AG, Kormoranweg 5, D-65201 Wiesbaden. Irrespective thereof N26 Bank GmbH may also transmit information concerning our outstanding claims against you to SCHUFA. This is permissible according to the German Data Protection Act (Section 28a, Subsection 1, Sentence 1) if I you have not paid the due amount irrespective of the fact it has fallen due for payment; the forwarding is necessary to safeguard legitimate interests of N26 or third parties and the claim is enforceable or you have expressly acknowledged the claim or after the claim fell due for payment you received at least two written reminders, N26 informed you in good time, at the earliest, however, by way of the first reminder, of the pending forwarding after four weeks at least, and you have not contested the claim, or the contractual relationship

underlying the claim may be terminated without notice by N26 on the basis of payment arrears, and if N26 has informed you of the pending forwarding.

Furthermore, N26 shall also transmit data about other conduct that is not as per agreement (e.g. account or credit card misuse or other fraudulent acts) to SCHUFA. Such notification may only be provided in accordance with the German Data Protection Act (Section 28, Subsection 2) insofar as this is necessary to safeguard legitimate interests of N26 or third parties, and there is no reason to assume that the interest of the affected parties that is worthy or protection overrides the exclusion of such forwarding.

To this extent, you release N26 Bank GmbH from the obligation of banking secrecy.

SCHUFA stores and uses the data received. The use also includes calculating a probability value based on the SCHUFA dataset to assess the credit risk (score). It forwards the received data to its contractual partners in the European Economic Area and Switzerland to provide such parties with information on assessing the creditworthiness of natural persons. Contractual partners of SCHUFA are companies that are subject to financial default risks based on their underlying services or deliveries (particularly credit institutions as well as credit card and leasing companies, but also letting, trading, telecommunications, energy supplying, insurance and collection companies). SCHUFA only makes personal data available if a legitimate interest in that respect has been credibly presented, and if the forwarding is permissible following consideration of all interests. Accordingly, the scope of the respective data made available may vary depending on the type of contractual partner. Furthermore, SCHUFA uses the data for the examination of identity and age of persons upon request from its contractual partners, who, for example offer services on the internet.

You are entitled to receive information about stored data concerning yourself from SCHUFA. Further information about the SCHUFA information and scoring procedure can be viewed at www.meineschufa.de. SCHUFA postal address is: SCHUFA Holding AG, Privatkunden ServiceCenter, post office box 103441, D-50474 Cologne.

Consent to Clause 8 applies only for customers who sign up with an address in Germany only applies to you if you have an address in Germany.

9. Term of contract; Termination

9.1

Your contractual relationship with us runs indefinitely. It ends automatically with the end of your contract for the current account offered by us and administered with the App and the Online Interface, if nothing else has been agreed to with you. With the end of our contractual relationship with you, all of the rights of use granted to you in accordance with these Supplementary Provisions likewise end.

9.2 End User's right of termination

The termination rights of the Customer, Clause 18 of the General Business Conditions of N26; Basic Rules Governing the Relationship Between the Customer and the Bank are taken as agreed.

9.3 Termination right of N26

The termination rights of the Bank, Clause 19 of the General Business Conditions of N26; Basic Rules Governing the Relationship Between the Customer and the Bank are taken as agreed.

For Customers with the right to a basic payment account according to §38 et seq. of the Payment Accounts Act (§ 38 ff. Zahlungskontengesetz – ZKG, only available in German), contrary to Sentence 1 the termination right in accordance with § 42 Paragraph 2 of the Payment Accounts Act (§ 42 Absatz 2 ZKG, only available in German) is taken as agreed with the end Customer.

10. Liability

10.1

We shall be liable without restriction for damages arising from injury to life, limb or health, which rests on a breach of duty by us, a legal representative, or auxiliary of us, which are caused by the absence of guaranteed quality by us or malicious behaviour on the part of us, as well as for damages that were caused by premeditation or gross negligence on the part of us or of a legal representative or auxiliary of us.

10.2

In the event of a breach of significant contractual duties due to gross negligence, we shall be liable except in the cases listed in Clauses 10.1 and 10.3, with the amount to be limited to foreseeable damages typical under the contract. Significant contractual duties are abstractly those duties whose fulfilment makes it possible in the first place to implement a contract in orderly fashion, and upon whose observance the contractual parties may regularly rely.

10.3

Liability under the product liability law remains unaffected.

10.4

Otherwise liability on the part of N26 is excluded.

11. Set-off

You can only set off our claims with undisputed or legally established counter-claims.

12. Amendment of the supplementary provisions

12.1

We can only amend these Supplementary Provisions when the amendment is reasonable for you, taking into consideration our interests. We will inform you about an amendment at least two months before the time at which the amendments become effective by email (“amendment offer”) or by message to your inbox in the App and the Online Interface (Messages from N26). If you do not agree with the amendments, you can terminate the contract until the point of time the amendments take effect without any prior notice. Otherwise your consent is considered to have been given to the amendments with effect as of the point in time named in the communication of amendment. In the amendment offer, we will inform you about your right of termination as well as the timeframe for termination. Please note that in case of a termination, use of the current account through the App and the Online Interface will no longer be possible.

N26

12.2

For an amendment of the price list referenced in Clause 5 of these Supplementary Provisions, Clause 12.1 of these Supplementary Provisions applies accordingly.

13. Miscellaneous

For these Supplementary Provisions, German law applies to the exclusion of international private law. In the course of business with consumers inside the European Union, the law at the place of residence of the consumer can also be applied, if mandatory applicable consumer-related provisions are concerned.