Who Pays When Things Go Wrong? Online Financial Fraud and Consumer Protection in Scandinavia and Europe

MARTE EIDSAND KJØRVEN*

Abstract

Online financial fraud targeted at consumers through phishing attacks and identity theft, for example, is a growing problem. Because it can be difficult to recover losses from the person who committed the fraud, the loss will often remain with either the financial institution or the consumer. This paper's research question relates to how losses following online financial fraud are and should be allocated between these two parties according to relevant Scandinavian and European law. For payment-transaction fraud, questions of loss allocation are regulated by national rules implementing the liability regime for unauthorised payment transactions under the payment services directive. For other financial services, these questions are resolved according to general rules on contract and tort. The analysis shows that consumers are often left to deal with the losses caused by online financial fraud. It is argued that the digitalisation of the financial services industry has in practice led to a shift in who bears the risk for attacks against financial institutions. This conflicts with the EU's stated policy goals to provide strong consumer protection in the field of cybercrime. The paper concludes that a larger portion of the losses incurred from online financial fraud should be allocated to financial institutions.

A. Introduction

Financial services have been profoundly transformed by digitalisation in recent years. The financial sector is the largest user of digital technologies, representing a major driver in the digital transformation of society and the economy.[1] New technologies create opportunities to provide better and cheaper access to financial services. By using online solutions, consumers

* Marte Eidsand Kjørven is Associate Professor (PhD) in the Department of Private Law, University of Oslo, Norway. The author gave a talk on selected aspects of this paper at a seminar organised by Professor Gudula Deipenbrock at HTW Berlin, University of Applied Sciences, Germany, on 16 November 2018. The author is grateful to Professor Gudula Deipenbrock for the invitation.

[1] European Commission, Communication from the Commission to the European Parliament, the Council, the European Central Bank, the European Economic and Social Committee and the Committee of the Regions, FinTech Action plan: For a more competitive and innovative European financial sector, Com(2018) 109 final, 2 (8 March 2018).

Electronic copy available at: https://ssrn.com/abstract=3583369

can easily authorise payment transactions, make investments or sign credit agreements from the comfort of their homes. This is both time- and cost-efficient for financial service providers and their customers. However, while the digital revolution in the financial services industry has created greater opportunities, it has also resulted in an increase in cybercrime. A recent report on the economic impact of cybercrime estimates that the global cost may be as much as USD 600 billion.[2] This paper deals with the legal challenges related to the allocation of these losses.

The paper focuses on third-party online financial fraud, that is fraud relating to the online use of financial services. Consumers are particularly vulnerable to fraud and to the economic impact of such fraud. It is increasingly recognised that human links are easy targets in security chains.[3] Rather than attacking financial institutions directly, criminals can target consumers through authorised push payment scams, phishing attacks or identity theft, for example.[4] The goal of such consumer-targeted attacks is typically to deceive the consumer into revealing the security information that the fraudster needs to log in to the consumer's account or sign in his/her name. If successful, the fraudster can empty the victim's account, or obtain credit cards and loans in the victim's name. The fraudster will of course be liable for the resulting loss. However, because it can be difficult to recover losses from the person who committed the fraud, in practice the loss will often remain with either the financial services provider or the consumer. Hence, liability issues and the allocation of losses between these parties is a challenging issue.

This paper's research question is twofold. First, how do current rules on liability allocate losses resulting from third-party online financial fraud between consumers and financial service providers *de lege lata*?[5] The paper attempts to answer this question by reviewing the relevant Scandinavian (Danish, Swedish and Norwegian) and European law.[6] Second, should financial

[2] James Lewis, *Economic Impact of Cybercrime—No Slowing Down*, 28 (CSIS/McAfee Report, February 2018) https://csis-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf (call-off date for all hyperlinks, unless stated otherwise: 11 June 2019).

[3] Hossein Siadati, Toan Nguyen, Payas Gupta, Markus Jakobsson, Nasir Memon, *Mind Your SMSes: Mitigating Social Engineering in Second Factor Authentication* 65 Computers & Security 14, 14 (2017); Ayelet Avni, *Who's the Weakest Link When It Comes to Mobile Banking Fraud? We Are* (10 March 2016), https://securityintelligence.com/whos-the-weakest-link-when-it-comes-to-mobile-banking-fraud-we-are/.

[4] These forms of online financial fraud are further described below in section B.II.

[5] The paper will not discuss the allocation of losses between the different financial service providers involved.

[6] Denmark and Sweden are members of the EU, whereas Norway is an EEA member.

Electronic copy available at: https://ssrn.com/abstract=3583369

institutions bear the larger part of losses following from online financial fraud *de lege ferenda*, in order to achieve the political goal of strong consumer protection in cases of cybercrime on the financial market?

The paper starts by describing the problem of consumer-targeted online financial fraud in section B. This section also provides insight into the policy goals of the digital single market for financial services, including the goal of consumer protection against cyber-related crime. Sections C and D consider how losses are allocated under Scandinavian law between financial service providers and consumers after payment transaction fraud and fraud related to credit contracts respectively. Directive (EU) 2015/2366 on payment services in the internal market [hereinafter, PSD 2][7] establishes a detailed regime for loss allocation between the payment service provider and the consumer following unauthorised payment transactions. Hence, for fraud related to payment services, questions of loss allocation are mainly regulated by the national rules implementing this liability regime.[8] For other financial services, questions of liability and loss allocation following fraud are not regulated under European law. In Scandinavian countries, these questions are resolved by applying general rules of contract and tort. The paper focuses on credit agreements because the case law indicates that fraud is widespread in this area. The analyses in Section D show that consumers are often held responsible for credit agreements concluded in their name by fraudsters.

In Section E, our focus turns to the *de lege ferenda* question, that is, whether financial institutions should shoulder a larger part of financial losses due to online fraud. It is argued that the digitalisation of the financial services industry has in practice led to a shift in who bears the risk for attacks against financial institutions, and that the consequences of this shift conflict with the policy goal of strong consumer protection for victims of cybercrime in the EU. The analysis of the liability regime for unauthorised payment transactions based on PSD 2 compared to the national regulation of liability for fraud in credit agreements shows how the lack of an overall EU-based regulatory framework can lead to dramatic inconsistencies in how losses

[7] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC [hereinafter, PSD 2], OJ L 337/35 (23 December 2015).

[8] See section C.I on how PSD 2 has been transposed into national law in the Scandinavian countries.

Electronic copy available at: https://ssrn.com/abstract=3583369

resulting from fraud are allocated for different financial services. Hence, the paper concludes that financial institutions should shoulder a more significant portion of the losses ensuing from online financial fraud.

B. The Problem: Consumer-Targeted Online Financial Fraud

I. Digitalisation and Protection of Consumers affected by the Resulting Increase in Cybercrime

As explained, the financial sector is the largest user of digital technologies and a major driver in the digital transformation of society and the economy.[9] The digitalisation of financial markets has been welcomed by the EU. The creation of the Digital Single Market for goods and services, including financial services, is considered a political priority for the European Parliament and the European Commission.[10] This is because achieving a Digital Single Market will ensure that Europe maintains its position as a world leader in the digital economy, helping European companies to grow globally.[11]

However, as our daily lives and economies have become increasingly dependent on digital technologies, we have become more and more exposed to criminal activities online. Cybercrime poses a serious threat to our economies. Unsurprisingly, the financial sector is the sector most under attack[12] and, as a result, improving cybersecurity is high on the EU's political agenda. In a joint communication to the European Parliament and the Council on cybersecurity in the EU,

[9] European Commission, Communication from the Commission to the European Parliament, the Council, the European Central Bank, the European Economic and Social Committee and the Committee of the Regions, FinTech Action plan: For a more competitive and innovative European financial sector, COM(2018) 109 final, 2 (8 March 2018).

[10] European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A Digital Single Market Strategy for Europe, COM(2015) 192 final (6 May 2015).

[11] European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A Digital Single Market Strategy for Europe, COM(2015) 192 final, 3 (6 May 2015).

[12] European Commission, Communication from the Commission to the European Parliament, the Council, the European Central Bank, the European Economic and Social Committee and the Committee of the Regions, FinTech Action plan: For a more competitive and innovative European financial sector, COM(2018) 109 final, 2 (8 March 2018).

Electronic copy available at: https://ssrn.com/abstract=3583369

the European Commission stated: 'we need a Europe that is resilient, which can protect its people effectively by anticipating possible cybersecurity incidents, by building strong protection in its structures and behavior'.[13] High levels of protection are important to ensure that trust in the digital market is maintained. But because the consequences of fraud in contracts for financial services can be personally and economically devastating, protection against such cybercrime is also a fundamental rights issue.[14] In particular, the European Commission emphasises that the Digital Single Market 'should offer EU citizens the same level of safety and the same expectations in online dealings that they have in their day-to-day offline life'.[15] The specific problems related to cybercrime in financial services are further addressed in the 2018 FinTech Action Plan.[16] Even though the financial sector is better prepared than other sectors, it is also the sector most under attack. The European Commission emphasises that cyber risks pose a mounting threat to the stability of the financial system and could undermine the confidence vital to financial markets. Recognising the potential threat to the financial sector's stability, the European Parliament has called on the European Commission 'to make cybersecurity the number one priority in the FinTech action plan'.[17]

[13] European Commission, Joint Communication to the European Parliament and the Council, Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU, Communication JOIN(2017) 450 final, 20 (13 September 2017).

[14] European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A Digital Single Market Strategy for Europe, COM(2015) 192 final, 12 (6 May 2015).

[15] European Commission, Commission Staff Working Document, A Digital Single Market Strategy for Europe - Analysis and Evidence Accompanying the document Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A Digital Single Market Strategy for Europe, SWD(2015) 100 final, 51 (6 May 2015).

[16] European Commission, Communication from the Commission to the European Parliament, the Council, the European Central Bank, the European Economic and Social Committee and the Committee of the Regions, FinTech Action Plan: For a more competitive and innovative European financial sector, COM(2018) 109 final (8 March 2018).

[17] European Commission, Communication from the Commission to the European Parliament, the Council, the European Central Bank, the European Economic and Social Committee and the Committee of the Regions, FinTech Action plan: For a more competitive and innovative European financial sector, COM(2018) 109 final, 16 (8 March 2018).

Electronic copy available at: https://ssrn.com/abstract=3583369

II. Forms of Consumer-Targeted Financial Fraud: The Role of Technology for Authentication and Electronic Signatures

The digital use of financial services, for example the initiation of payment transactions, depends on technology capable of identifying the customer. The electronic conclusion of a contract (a credit agreement, for example) also depends on online authentication systems and technologies that enable electronic signatures. As explained, the goal of consumer-targeted fraud in financial services typically includes deceiving the consumer into disclosing security information that the fraudster needs to authenticate or sign in the consumer's name.[18] The methods used to acquire the needed security information often include so-called social engineering. Social engineering is the art of persuading people to divulge sensitive information or to take certain courses of action.[19] Central to social engineering attacks is the abuse of the victim's trust. Instead of direct technical attacks on systems, social engineers target humans in order to gain access to confidential information.[20] Some common forms of consumer-targeted financial fraud are described in the following paragraphs.

The European Police Office (Europol) publishes an annual Internet Organised Crime Threat Assessment (IOCTA), which provides an update on the latest trends and the current impact of cybercrime within Europe and the EU. According to the 2018 IOCTA report,[21] social engineering is at the heart of many cybercrimes, and its importance is still growing.[22] According to the report, phishing via email remains the most frequent form of social engineering. Phishing

[18] Markus Jakobsson, *Two-Factor Inauthentication – The Rise in SMS Phishing Attacks*, 2018 Computer Fraud & Security 6, 6 (2018).

[19] Francois Mouton, Mercia M. Malan, Louise Leenen and H.S. Venter, *Social Engineering Attack Framework*, conference paper presented at 'Information Security for South Africa', Johannesburg, South Africa (August 2014).

[20] Katharina Krombholz, Heidelinde Hobel, Markus Huber and Edgar Weippl, *Advanced Social Engineering Attacks*, 22 Journal of Information Security and Applications 113, 114 (2015).

[21] Europol, *Internet Organised Crime Threat Assessment (IOCTA) 2018*, 8 (2018), https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018.

[22] A report from the Norwegian Financial Services Authority comes to the same conclusion in a national context: Norwegian Financial Conduct Authority, *Finansforetakenes bruk av informasjons- og kommunikasjonsteknologi (IKT) Risiko Og Sårbarhetsanalyse (ROS)*, 19 (8 May 2018), https://www.finanstilsynet.no/contentassets/a92eb0d064a94bcfa0b8d862936af02e/risiko--og-sarbarhetsanalyse-2018.pdf.

Electronic copy available at: https://ssrn.com/abstract=3583369

typically includes the use of a spoof email purporting to be from a legitimate actor (such as a bank) and designed to lead consumers to fraudulent websites, where they are tricked into delivering security information such as passwords.[23] Alternatively, the email may contain spyware or a link to a webpage containing spyware, which if run gives the fraudster access to security information when the consumer later logs in, for example, to their bank's website.

A related type of fraud is called vishing. 'Vishing' refers to social engineering fraud committed by means of phone calls to the victim. The fraudster typically calls the victim, posing as a trustworthy agent, such as the police or a bank. The fraudster then tells the consumer that they need to move or withdraw their money quickly to keep it safe,[24] or they trick the victim into handing over security information. In 2015, the British Financial Ombudsman conducted a review of vishing complaints received between 2012 and 2014.[25] The Ombudsman found that in total, the 185 complaints involved losses of approximately GBP 4.3 million. A fifth of the consumer victims had lost between GBP 20,000 and GBP 49,999 – but one in ten had lost more than that. The largest individual loss was over GBP 100,000.

So-called authorised push payments represent an increasingly popular method of consumer-targeted fraud. The term is commonly used to describe situations in which a fraudster tricks a consumer into transferring money to an account controlled by the fraudster.[26] A prominent example involves home buyers who are tricked by fraudsters posing as their conveyancing solicitors into transferring funds equivalent to the house's price to the fraudster.[27] According to the British Financial Ombudsman, there were 43,875 reported cases of authorised push payment

[23] Anti-Phishing Working Group, Phishing Activity Trends Report 4th quarter 2018, 2 (4 March 2019), http://docs.apwg.org/reports/apwg_trends_report_q4_2018.pdf.

[24] British Financial Ombudsman Service, *Calling Time on Telephone Fraud: A Review of Complaints about "Vishing" Scams* (July 2015), https://www.financial-ombudsman.org.uk/news/updates/vishing-report-2015.html.

[25] British Financial Ombudsman Service, *Calling Time on Telephone Fraud: A Review of Complaints about "Vishing" Scams* (July 2015), https://www.financial-ombudsman.org.uk/news/updates/vishing-report-2015.html.

[26] See, for example, British Financial Conduct Authority, *Authorised Push Payment Fraud - Extending the Jurisdiction of the Financial Ombudsman Service*, CP18/16, 5 (June 2018), https://www.fca.org.uk/publication/consultation/cp18-16.pdf.

[27] As described in the media: BBC News, *Refund Hopes Rise for Payment Scam Victims* (28 September 2018) https://www.bbc.com/news/business-45664980.

Electronic copy available at: https://ssrn.com/abstract=3583369

scams in the UK in 2017, resulting in total losses of GBP 236 million. Consumers represented 88% of the victims.[28]

Phishing, vishing and authorised push payments are methods typically used by a fraudster unknown to the victim. However, fraud can also be committed by family or friends, commonly called familiar fraud. The evolution in Scandinavian case law suggests that familiar fraud is a growing problem and that these situations raise difficult questions of liability.[29] For a family member living in the same household as the consumer, it is fairly easy to gain access to the personal information needed, for example, to initiate payment transactions in the consumer's name. Common examples of familiar fraud include a daughter or son misusing a parent's security information under the cover of helping them pay bills, or a spouse misusing his or her partner's security information to secretly conclude a credit agreement in the partner's name.

A distinction can be made between fraud involving authentication processes linked to a particular financial service provider, on the one hand, and fraud involving the collection of security information needed to misuse a third-party authentication scheme, on the other. Third-party authentication schemes are systems for electronic identification, and multiple providers may use the same third-party scheme. The Norwegian authentication scheme, called BankID, and similar systems used in Sweden and Denmark are further described in section B.III. The consequences of the misuse of a third-party identification scheme are typically more far-reaching than the misuse of authentication procedures linked to a particular financial service provider. For example, if a phishing attack gives the fraudster access to specific credit card details, the credit card can be used to make unauthorised payment transactions. However, if a consumer is tricked into disclosing his or her security credentials for a general identification scheme, the fraudster could authenticate as the victim with every provider that accepts this third-party scheme for authentication. If successful, the latter represents what might be considered complete identity theft, resulting in unlimited opportunities for fraud.[30] According

[28] British Financial Conduct Authority, *Authorised Push Payment Fraud - Extending the Jurisdiction of the Financial Ombudsman Service*, CP18/16, 5 (June 2018), https://www.fca.org.uk/publication/consultation/cp18-16.pdf.

[29] See section D.

[30] The term 'identity theft' has no clear definition. The Organisation for Economic Co-operation and Development (OECD), has proposed the following definition of identity theft: 'Identity theft occurs when a party acquires, transfers, possesses or uses personal information of a natural or legal person in an unauthorised manner

Electronic copy available at: https://ssrn.com/abstract=3583369

to a study carried out on behalf of the European Commission, identity-theft-related crime affects a considerable proportion of the population and is on the rise.[31] The report estimates that as many as 8.2 million individuals (2% of the EU's population) are affected by identity theft, with an average loss of around EUR 2,500. Whereas the consequences of a single fraud attack are limited in most cases, a fraudster who achieves complete identity theft can leave the victim in financial (and personal) ruin.

III. The Norwegian Authentication Scheme (BankID) and Similar Swedish and Danish Systems

As explained above, consumer-targeted online fraud often involves the misuse of authentication and electronic-signature technology. The financial industry in Scandinavian countries was an early adopter of digital solutions and services. Digital innovation through new identification technologies was of particular importance to the early digitalisation of financial services. But this development has also occasioned rather widespread problems of fraud.[32] In a recent newspaper article, the Norwegian Police Service stated that because identification-technology fraud related to financial services provides high returns, it will soon become more popular than drug dealing among criminals in Norway.[33] For the international reader, a short explanation of how Scandinavian electronic identity systems work and how they can be misused in the context of online financial services may be useful.

---

with the intent to commit, or in connection with, fraud or other crimes.' See OECD, *OECD Policy Guidance on Online Identity Theft*, 2 (2008), http://www.oecd.org/sti/consumer/40879136.pdf.

[31] European Commission Directorate General for Home Affairs, *Study for an Impact Assessment on a Proposal for a New Legal Framework on Identity Theft* (2012), https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/policies/organized-crime-and-human-trafficking/cybercrime/docs/final_report_identity_theft_11_december_2012_en.pdf.

[32] See cases referred to in sections C and D. For more information on security weaknesses in the BankID system, see Kristian Gjøsteen, *Weaknesses in BankID, a PKI-Substitute Deployed by Norwegian Banks*, in Mjølsnes S.F., Mauw S., Katsikas S.K. (eds) *Public Key Infrastructure. EuroPKI 2008*, vol 5057, 196 (Berlin: Springer, 2008); Yngve Espelid, Lars-Helge Netland, Andre N. Klinsheim and Kjell J. Hole, *Robbing Banks with Their Own Software—an Exploit Against Norwegian Online Banks*, in Jajodia S., Samarati P., Cimato S. (eds) *Proceedings of the IFIP TC 11 23rd International Information Security Conference* 64 (IFIPAICT vol 278, Springer 2008).

[33] Ådne Husby Sandnes, *Gjengmiljø mistenkt for grov utpressing: Kjøpte dyre biler og leilighet* (2 April 2019), https://www.vg.no/i/8wy34A.

Electronic copy available at: https://ssrn.com/abstract=3583369

The development of the Norwegian electronic identity scheme BankID began in 2000. The first customers implemented BankID in 2004 and it is currently used by approximately 4 in 5 Norwegians.[34] The BankID system is used both as a digital identification tool and as a means of creating legally binding digital signatures. All of the country's banks, many public sector service providers, and an increasing number of businesses in a wide range of sectors use BankID. Norwegians can use the BankID system to apply for a range of public sector services, to access their digital health data, to report to the tax authorities, to verify payments, to bid on real estate, to sign tenancy agreements, to change electricity suppliers, to access Digipost (Norway Post's national digital mailbox), to report a change of address, to register a divorce and many other things.[35] The wide range of areas in which Norwegians may use BankID to access important services explains the extremely high number of Norwegian adults who use the system. Those who are excluded from the system are mainly children and groups of citizens that for other reasons cannot access a BankID account.

The practical use of BankID requires a physical code device, an app or so-called BankID on mobile. With an app or code device, BankID users can identify themselves using their social security number and a one-off code provided by their code unit or app, together with a personal password. With BankID on mobile, the BankID is stored on the mobile's SIM card, and authentication is performed using the mobile number, the birthdate and a PIN-protected process on the mobile phone. Both Denmark and Sweden have similar identification schemes. The Swedish system is called BankID as well (though it is a different scheme). In Denmark, the identification scheme is called NemID. NemID requires a username, personal password and one-time password. The one-time password appears on a credit-card-sized paper card and consists of six digits. There are alternative identification schemes in each of the Scandinavian countries, but NemID and the BankID systems are by far the most commonly used. The authentication schemes use so-called two-factor authentication. Online authentication typically includes the use of one or more of the three elements: knowledge (something only the user knows, such as a password or PIN), possession (something only the user possesses, such as a mobile phone or credit card) and inherence (something that uniquely identifies the user, such as fingerprints or facial features). Generally, authentication schemes that combine two or more

[34] BankID, https://www.bankid.no/en/private/about-us/.

[35] BankID, https://www.bankid.no/en/private/areas-of-use/.

Electronic copy available at: https://ssrn.com/abstract=3583369

of these elements are more secure than those that use only one. As the term indicates, two-factor authentication is an authentication process based on two of the aforementioned elements.

Two-factor authentication corresponds to what Article 4 Section 30 of PSD 2 classifies as strong customer authentication. According to Article 97 of PSD 2, payment service providers are generally required to use strong customer authentication for electronic payment transactions.[36] Although two-factor authentication is more secure than one-factor authentication, it still cannot fully prevent the consumer-targeted fraud methods described above.[37] The main objective of two-factor authentication is to build a second layer of authentication that can be used even when a user's credentials are known to a fraudster.[38] However, by using social engineering methods, the fraudster can rather easily trick the user into handing over the second-layer verification code. For example, if a user is directed to a phishing website and enters his or her credentials, the hacker can use those credentials to log in to the legitimate website. A one-time code is then sent to the user's device and the user enters that code into the phishing website. The attacker then uses the code on the legitimate webpage.[39] Studies have shown that such phishing attacks have achieved high success rates against websites using two-factor authentication. Siadati and others reported a social engineering attack in which the attacker was able to trick as many as 50% of users into forwarding their second-layer verification code.[40]

[36] The requirements for strong customer authentication are further specified in European Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication, OJ L 69/23 (13 March 2018).

[37] Hossein Siadati, Toan Nguyen, Payas Gupta, Markus Jakobsson, Nasir Memon, *Mind Your SMSes: Mitigating Social Engineering in Second Factor Authentication* 65 Computers & Security 14, 26 (2017).

[38] Hossein Siadati, Toan Nguyen, Payas Gupta, Markus Jakobsson, Nasir Memon, *Mind Your SMSes: Mitigating Social Engineering in Second Factor Authentication* 65 Computers & Security 14, 14 (2017).

[39] Titanadmin, *Does 2-Factor Authentication Stop Phishing Attacks?* (SpamTitan, 10 January 2019), https://www.spamtitan.com/blog/does-2-factor-authentication-stop-phishing-attacks/. Recently, a new tool has been developed, automating the phishing of one-time passcodes, see John E Dunn, *2FA Codes Can Be Phished by New Pentest Tool* (Naked Security, 11 January 2019), https://nakedsecurity.sophos.com/2019/01/11/2fa-codes-can-be-phished-by-new-pentest-tool/.

[40] Hossein Siadati, Toan Nguyen, Payas Gupta, Markus Jakobsson, Nasir Memon, *Mind Your SMSes: Mitigating Social Engineering in Second Factor Authentication* 65 Computers & Security 14, 26 (2017).

Electronic copy available at: https://ssrn.com/abstract=3583369

As early as 2005, tech guru Bruce Schneier wrote that two-factor authentication 'won't defend against phishing. It's not going to prevent identity theft. It's not going to secure online accounts from fraudulent transactions. It solves the security problems we had 10 years ago, not the security problems we have today.'[41] Two-factor authentication is unsuitable for preventing fraud in close relations as well.[42] A consumer's password can be detected fairly easily by those living in the same household and the possession (e.g. the device on which a one-time code appears) is easily accessible by family members.

The mutual recognition of electronic identity schemes like BankID and NemID across Europe is mandated by Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market [hereinafter, eIDAS Regulation],[43] which also includes rules on the recognition of electronic signatures.[44] The regulation seeks to enhance trust in electronic transactions in the internal market by providing a common foundation for secure electronic transactions.[45] The eIDAS Regulation includes rules on liability for the trust services provider for damage caused due to failure to comply with technical specifications, standards and procedures.[46] However, the consumer-targeted forms of fraud discussed in this article typically happen because the consumer makes mistakes regarding security. This paper will not discuss liability questions in situations where the loss results from a lack of compliance with technical standards. Hence, the liability rules under the eIDAS Regulation will not be further discussed.

[41] Bruce Schneier, *Two-Factor Authentication: Too Little, Too Late* (April 2005), https://www.schneier.com/essays/archives/2005/04/two-factor_authentic.html.

[42] Markus Jakobsson, *Two-Factor Inauthentication – The Rise in SMS Phishing Attacks*, 2018 Computer Fraud & Security 6, 6 (2018).

[43] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [hereinafter, eIDAS Regulation], OJ L 257/73 (28 August 2014).

[44] Article 25, eIDAS Regulation.

[45] Recital (2), eIDAS Regulation.

[46] Articles 11(2) and 7(e), eIDAS Regulation.

Electronic copy available at: https://ssrn.com/abstract=3583369

C. Consumer Liability for Payment-Transaction Fraud

I. Introduction

Rules on liability and loss allocation for payment transaction fraud were first introduced at the European level in the Payment Services Directive 2007/64/EC[47] [hereinafter, PSD 1]. In order to encourage electronic payment solutions, liability for unauthorised payment transactions lay, in the main, with the payment service provider.[48] PSD 2 was enacted in 2015 and came into effect in the EU on 13 January 2018. The liability regime remains essentially the same under PSD 2, but with some additional protection for consumers.[49] When transposed into national law, full harmonisation is demanded as a main rule.[50] In Sweden and Denmark, PSD 2 has been transposed into national law and is now in force.[51] In Norway, PSD 2 has not yet been fully implemented.[52] It was incorporated into the EEA Agreement 14 June 2019.[53] In Norway, the main rules on liability for unauthorised payment transactions still follow from the national rules implementing the liability regime under PSD 1.[54] Because the parts of the liability regime discussed in this paper remain essentially the same under PSD 2, this has limited practical importance for the discussions here.

[47] 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 [hereinafter PSD 1], OJ L 319/1 (5 December 2007).

[48] Article 60, PSD 1.

[49] See section C.II.

[50] Article 107, PSD 2.

[51] The liability regime under PSD 2 has been implemented into Swedish law in a new chapter 5a in Act 2010:75 on Payment Services and in Denmark in section 92-101 of Act 8. June 2017 nb. 652 on Payments.

[52] As a member of the EEA, EU legislation must be incorporated into the Agreement on the European Economic Area (EEA Agreement) and subsequently transposed into Norwegian law. Both regulations and directives must be implemented in Norwegian law. Regulations do not have direct effect in national law in the EEA countries.

[53] EEA Joint Committee Decision No 165/2019. Though not formally obliged to do so, the Norwegian Ministry of Justice and Public Security requested comments on a proposal for a new act on contracts for financial services in the autumn of 2017, implementing the private law aspects of PSD 2. The work is still ongoing. In order to ensure a level playing field within the Norwegian financial industry, some of the private law aspects of PSD 2 have been given effect in Norwegian law through a temporary administrative regulation: Regulation 18. February 2019 nb. 135 on Payment Services.

[54] Norwegian Act 25 June 1999 nb. 46 on Contracts for Financial Services.

Electronic copy available at: https://ssrn.com/abstract=3583369

PSD 2 sets out a detailed liability regime for unauthorised payment transactions, with the main rules following from Articles 73 and 74. In the following, section C.II will give a brief overview of this liability regime.[55] Then, in section C.III, three important concepts adopted by this liability regime will be explored, including how these concepts have been implemented and applied in the Scandinavian countries. The discussion will provide insight into how losses are allocated between the payment services provider and consumers in specific situations of payment-transaction fraud, including authorised push payment scams, phishing and vishing attacks and familiar fraud.

II. Overview of the PSD 2 Liability Regime

The main rule introduced in PSD 1, that the payment services provider is liable for loss after an 'unauthorised payment transaction', has remained the same under PSD 2.[56] A payment transaction is considered to be authorised only if the payer has given consent to execute the payment transaction.[57] Consent must be given in the form agreed upon between the payer and the payment service provider. Conversely, a payment transaction is unauthorised in the absence of consent. The concept of an 'unauthorised payment transaction' will be further explored in section C.III.1.

If the loss relates to a lost, stolen or misappropriated payment instrument,[58] the payer is liable for an individual share of EUR 50 according to Article 74 Section 1 first paragraph of PSD 2. The individual share under Article 74 Section 1 of PSD 2 does not apply if the misuse was not detectable to the payer or if the loss was caused by a representative of the payment service provider. Under PSD 1, the individual share was EUR 150, and it applied to all situations where

[55] For more thorough discussions on the liability regime under PSD 2 as compared to the liability regime under PSD 1, see Reinhard Steennot, *Reduced Payer's Liability for Unauthorized Payment Transactions under the Second Payment Services Directive (PSD2)* 34 Computer Law & Security Review 954, 962 (2018).

[56] Article 73(1), PSD 2 and Article 60(1), PSD 1.

[57] Article 64(1), PSD 2 and Article 54(1), PSD 1.

[58] 'Payment instrument' is defined in Article 4(14) of PSD 2 as a 'personalised device(s) and/or set of procedures agreed between the payment service user and the payment service provider and used in order to initiate a payment order'. The wording is the same as that previously used under Article 4(23) of PSD 1. In Case C-616/11, *T-Mobile Austria GmbH vs. Verein für Konsumenteninformation* [2014] OJ C 175/04, the European Court of Justice decided that 'the procedure for ordering transfers through online banking constitute payment instruments' in the meaning of PSD 1. Hence when using authentication schemes like BankID to authenticate payment transactions, these procedures are considered a 'payment instrument' under PSD 1 and PSD 2.

Electronic copy available at: https://ssrn.com/abstract=3583369

loss occurred as a result of 'the use of a lost or stolen payment instrument'.[59] Hence, PSD 2 provides for enhanced consumer protection in this regard.

According to Article 74 Section 1 of PSD 2, the 'payer shall bear all of the losses relating to any unauthorised payment transactions if they were incurred by the payer acting fraudulently or failing to fulfil one or more of the obligations set out in Article 69 with intent or gross negligence.'[60] Article 69 of PSD 2 includes an obligation to use the payment instrument in accordance with the contract terms.[61] The contract terms may, for example, place an obligation on the customer to undertake a number of security measures, including updating antivirus software and other security-related software and keeping the computer's operating system and web browser updated. A consumer who fails to fulfil such obligations may be vulnerable to liability claims.[62] In addition to complying with contract terms, the customer is under a specific obligation to take all reasonable steps to keep personal security credentials safe.[63] In situations of fraud targeting consumers, the question of whether the consumer incurred the loss as a result gross negligence or intent is an important one. The concepts of gross negligence and intent in this relation will be further explored below, in sections C.III.2 and C.III.3.

The main rule on liability under PSD 2 is that customers are liable for the entire loss when acting fraudulently,[64] or when contractual obligations have been breached with intent or gross negligence.[65] However, the directive allows Member states to reduce liability for customers who have acted merely with gross negligence.[66] In Sweden customers are liable for up to SEK 12,000 (approximately EUR 1100),[67] while the amount in Denmark is DKK 8000 (approximately EUR 1000).[68] In Norway, the rules implementing PSD 1 are, as explained, still

[59] Article 60(1), PSD 1.

[60] The same followed from Article 61(2), PSD 1.

[61] Article 69(1)a, PSD 2. The same followed from Article 56(1), PSD 1.

[62] Nicole S van der Meulen, *You've Been Warned: Consumer Liability in Internet Banking Fraud* 29 Computer Law & Security Review 713, 715 (2013).

[63] Article 69(2), PSD 2 and Article 56(2), PSD 1.

[64] This paper focuses on questions of loss allocation following fraud committed by third parties. Hence, the concept of fraudulent behaviour on the part of the consumer will not be further discussed.

[65] Article 74(2), PSD 2.

[66] Article 74(2), PSD 2 and Article 61(3), PSD 1.

[67] Chapter 5a on unauthorised payment transactions, section 3, of Swedish Act (2010:751) on payment services.

[68] Danish Act 8 June 2017 nb 652 on payments, section 100.

Electronic copy available at: https://ssrn.com/abstract=3583369

in force, and customer liability is limited to NOK 12,000 (approximately EUR 1200) in these situations.[69] The payment service provider is under no circumstances liable for losses caused by payers acting fraudulently or failing to fulfil their obligations with intent.

A new rule under Article 74 Section 2 of PSD 2 states that in cases in which the payment service provider does not require strong customer authentication,[70] the payer shall not bear any financial losses unless they have acted fraudulently. Hence, even when the customer fails to comply with his or her obligations with intent or gross negligence, the payment service provider is liable. As explained, strong customer authentication implies authentication based on the use of two or more elements among knowledge, possession and inherence.[71] In the Scandinavian countries, the most common authentication schemes have used two factor authentication for a long time already. As explained in section B.III, such authentication cannot prevent common forms of consumer-targeted fraud such as phishing attacks or familiar fraud. The discussion in section C.III is based on the assumption that strong customer authentication is used.

The liability regime under PSD 2 also includes rules on the burden of proof. This is important in practice, because in situations of fraud it can be difficult for both the financial institution and the consumer to provide evidence of how the fraud occurred. Article 72 of PSD 2 states that when a payment service user denies having authorised an executed payment transaction, it falls to the payment service provider to prove that the payment transaction was authenticated, accurately recorded, entered in the accounts and not affected by a technical breakdown or some other deficiency of the service provided by the payment service provider. The article further specifies that the core use of a payment instrument is not in itself sufficient to prove either that the payment transaction was authorised or that the customer acted with intent or gross negligence. These rules on the burden of proof were the same under Article 59 of PSD 1. However, Article 72 Section 2 of PSD 2 includes a further specification, namely that the payment service provider shall provide supporting evidence to prove fraud or gross negligence on the part of the payment service user. In the recitals, the background to this new rule on the burden of proof with respect to negligence is explained by reference to the customer's limited

[69] Norwegian Act 25 June 1999 nb. 46 on Contracts for Financial Services, section 35.

[70] According to Article 97 of PSD 2, payment service providers must apply strong customer authentication for electronic payment transactions as a general rule.

[71] Article 4(30), PSD 2.

Electronic copy available at: https://ssrn.com/abstract=3583369

opportunity to provide evidence in cases of, for example, online-payment fraud.[72] It is too early to say whether the new specification in Article 72 Section 2 of PSD 2 will be of practical importance in Scandinavian countries.[73]

The liability regime under PSD 2 has been amended to include new payment services covered by the directive. In particular, if a payment initiation service provider is involved in the transaction, Article 73 Section 2 of PSD 2 implies that the account servicing payment service provider will be liable towards the payer. Rules on the allocation of losses between the different payment service providers are included as a result. Because this paper focuses on the allocation of losses between consumers on the one hand, and financial institutions on the other, these parts of the liability regime will not be further discussed.

III. Liability in Specific Situations of Payment-Transaction Fraud

1. The Concept of 'Unauthorised Payment Transaction' in Light of Authorised Push Payment Scams

As explained in section B.II, the term 'authorised push payments' describes a situation in which a fraudster tricks a payer into transferring money to an account controlled by the fraudster. Such scams can be accomplished by different means, including fake invoices or fraudulent phone calls. As the term implies, such payments are normally considered authorised. This is because the payment service provider has a duty to execute the payment transaction in accordance with the instructions given by the customer.[74] In fact, Article 89 of PSD 2 (corresponding to Article

[72] Recital 72, PSD 2.

[73] In Denmark, the rules on the burden of proof under PSD 2 are implemented word for word in Act 8 June 2017 nb 652 on Payments, section 98. In Sweden, these rules are not implemented explicitly in law. In the preparatory works implementing PSD 2 in Swedish law, the lawmaker announced that the Swedish rules on the burden of proof were already in line with the rules under PSD 2, see Government proposition Prop. 2017/18:77 Nya regler om betaltjänster, 165-166. In Norway, the new rules on the burden of proof have not yet been implemented. The rule under Article 59 of PSD 1, which corresponds to Article 72 (1) first paragraph and 72 (2) first sentence of PSD 2, are implemented in Norwegian Act 25 June 1999 nb. 46 on Contracts for Financial Services. Rules on the burden of proof will not be further discussed. See Reinhard Steennot, *Reduced Payer's Liability for Unauthorized Payment Transactions under the Second Payment Services Directive (PSD2)* 34 Computer Law & Security Review 954, 962 (2013), for more on the new rule on the burden of proof under Article 74 of PSD 2.

[74] Articles 88 and 89, PSD 2 (corresponding to Articles 74 and 75, PSD 1). See also British Financial Ombudsman Service, *Calling Time on Telephone Fraud: A Review of Complaints about "Vishing" Scams* (July

Electronic copy available at: https://ssrn.com/abstract=3583369

75 of PSD 1), stipulates that the payment service provider is liable to the payer for the correct execution of the payment transaction. Thus, a payment made according to customer instructions is 'authorised' and correctly executed when completed in accordance with information given by the consumer, even when the payer has been manipulated by a third party into giving such instructions.

In cases of authorised push payment fraud, the transaction is typically executed against the account number provided by the payer but to a payee other than that designated by the payer. Thus the transaction is in fact correctly executed only in part. However, it follows from Article 88 of PSD 2 that if 'a payment order is executed in accordance with the unique identifier, the payment order shall be deemed to have been executed correctly with regard to the payee specified by the unique identifier'. The same followed under Article 74 of PSD 1. The unique identifier is typically the account number. Hence, with respect to the information given by the payer, the payment service provider needs only to ensure that the transaction goes to the account number provided. A relevant example from the Norwegian Dispute Resolution for Financial Services body involves a consumer who received what was originally an authentic invoice from the contractor to whom he owed money following a renovation project.[75] However, a fraudster managed to change the account number on the invoice. The case was resolved under the Norwegian Financial Services Act, implementing rules under PSD 1.[76] As explained, these correspond to the rules under PSD 2. The consumer's argument that the payment order had not been executed correctly when the bank did not ensure that the name of the payee corresponded to the owner of the account number given was rejected.

2015), https://www.financial-ombudsman.org.uk/news/updates/vishing-report-2015.html, where the Financial Ombudsman stated that there was a long-established principle that banks are generally obliged to carry out their customers' instructions, leading to the conclusion that a payment made according to customer instructions is 'correctly made' even if the payer has been tricked by a third party into giving those instructions.

[75] Norwegian Consumer Dispute Resolution on Financial Services, BKN-2010-151. See also example from the Danish Consumer Dispute Resolution for Financial Services, Case 24/2018. Examples of cases are also given in British Financial Ombudsman Service, *Case 116/08*, Ombudsman News, Issue 116, 12 (March/April 2014), https://www.financial-ombudsman.org.uk/publications/ombudsman-news/116/issue116.pdf.

[76] Norwegian Financial Services Act, section 43.

Electronic copy available at: https://ssrn.com/abstract=3583369

An instance of push payment fraud can be very sophisticated.[77] But because the transactions are viewed as authorised under these circumstances, the consumer is fully liable for any loss, and there are no legal grounds for an allocation of losses from the consumer to the payment service provider. PSD 2 does impose some obligations on the payment service provider in situations in which the consumer is the victim of an authorised push payment scam. If the account details or other information about the payee provided by the payer are incorrect, the payer's payment service provider and the payee's payment service provider must cooperate to recover the funds involved in the transaction.[78] The directive does not provide for any liability rules in the event of the payment service provider's non-compliance with this obligation. The payment service provider might, however, be liable according to national rules of tort in situations in which it could have done more to reclaim the funds.[79]

2. The Concept of 'Gross Negligence' in Light of Phishing and Vishing Attacks and Familiar Fraud

As explained, consumer-targeted online financial fraud often involves tricking customers into giving away security information, enabling the fraudster to initiate a payment transaction from the victim's account. Transactions made by a fraudster using stolen security credentials are, under Article 64 of PSD 2, unauthorised. However, in such situations, the consumer has failed to keep his or her security credentials safe. If gross negligence is involved, the main rule under Article 74 Section 4 of PSD 2 is that the consumer is liable for the resulting loss. Hence, the concept of 'gross negligence' is an important one.

---

[77] British Financial Ombudsman Service, *Case 116/08*, Ombudsman News, Issue 116, 12 (March/April 2014), https://www.financial-ombudsman.org.uk/publications/ombudsman-news/116/issue116.pdf. Case study 116/08 shows just how sophisticated these scams can be. The case relates to a consumer receiving a phone call claiming to be from her bank. The person said there had been some suspicious activity on her account and told her to call the number on the back of her credit card. She hung up and called the number on the back of her card. The fraudster had put a technical fix in place so that when the consumer rang the number on the back of her card, she would be reconnected with the fraudster. She then followed the instructions she believed to be from her bank and transferred her money straight to the fraudster. The Financial Ombudsman concluded that since the consumer made the transfer herself there was no unauthorised access to her account and the bank was not liable.

[78] Article 88(3), PSD 2.

[79] To my knowledge, there are no examples from the Scandinavian countries of payment services providers being held liable on these grounds.

Electronic copy available at: https://ssrn.com/abstract=3583369

According to the recitals[80] in PSD 2, the evidence and degree of the alleged negligence should generally be evaluated according to national law.[81] However, Recital 72 of PSD 2 states that although the concept of negligence implies a breach of a duty of care, gross negligence must be more significant than mere negligence, involving conduct exhibiting substantial carelessness. As an example of gross negligence, the recital refers to storing the credentials used to authorise a payment transaction alongside the payment instrument in a format that is open and easily detectable by third parties. With the exception of this statement, the directive provides no further guidelines for the assessment of gross negligence.[82]

The wording of the national rules in Scandinavian countries gives no further guidance on how to interpret the concept of 'gross negligence' in this context.[83] Decisions by courts and alternative dispute resolution bodies diverge on the question of whether falling for a phishing attack constitutes gross negligence on the part of the consumer.[84] The Danish Consumer

[80] Recitals are an essential component in the interpretation of EU Directives and Regulations, see Llio Humphreys, Cristiana Santos, Luigi di Cargo, Guido Boella, Leon van der Torre and Livio Robaldo, *Mapping Recitals to Normative Provisions in EU Legislation to Assist Legal Interpretation*, in Antonino Rotolo (ed), *Legal Knowledge and Information Systems* (Amsterdam, Berlin, Washington DC: IOS Press, 2015) with further references.

[81] Recital 72, PSD 2.

[82] Examples of how the concept of gross negligence is understood in the Scandinavian countries are given in section C.III.

[83] Swedish Act on Payment Services, Chapter 5a, section 3; Danish Act on Payments, section 100(4); Norwegian Act on Contracts for Financial Services, section 35 (implementing the same rule contained in Article 61, PSD 1). In Norway, the concept of gross negligence in relation to keeping security credentials for payment instruments safe has been fleshed out in a Supreme Court case from 2004: Norwegian Supreme Court case, 19 March 2004, Rt. 2004 s. 499. However, the judgement does not specify the concept any further than the PSD 2 recitals. The Supreme Court concluded that keeping a payment card in a locked suitcase in a locked apartment together with a note book with the PIN camouflaged as a phone number was not grossly negligent. The Supreme Court argued that gross negligence implies exhibiting a significant degree of carelessness: *'grov uaktsom oppførsel må representere «et markert avvik fra vanlig forsvarlig handlemåte»'*.

[84] Most of the decisions relate to national rules implementing Article 61(2), PSD 1. As explained, the rules on consumer liability after a grossly negligent breach of obligations were the same under the previous directive and the national rules in Scandinavian countries have not changed either. In Sweden, Article 61 of PSD 1 was implemented in the now revoked Act (2010:738) on unauthorised payment transactions, section 6. This corresponds to the current rule under the Swedish Act (2010:751) on Payments, chapter 5a, section 3, which corresponds to Article 74(1) of PSD 2. In Denmark, Article 61 of PSD 1 was implemented in the now revoked

Electronic copy available at: https://ssrn.com/abstract=3583369

Dispute Resolution body has dealt with a number of cases regarding phishing.[85] The most recent case concerned a woman who received an email purporting to be from Nets, stating that her card would be debited for a large amount unless she cancelled the transaction. Believing that she was cancelling a fraudulent transaction, the woman gave her payment card details and SMS verification codes to the phishing website. This was not viewed as grossly negligent according to the national Danish rules implementing PSD 2.[86]

The Norwegian Consumer Dispute Resolution on Financial Services has taken a different view. In several dispute resolution cases, it has concluded that following a link in an email and then typing security information into the website to which the link leads constitutes gross negligence.[87] In a 2017 case, a consumer had received an email purporting to be from Apple and asking the consumer to confirm his account details.[88] The email included a link that led the consumer to a fake but realistic Apple ID website. After entering his Apple ID, the victim was directed to a second fake webpage, which asked the consumer to identify himself using BankID. [89] The Norwegian Consumer Dispute Resolution concluded that it was almost impossible for the consumer to see that the email and webpages were fake. However, it was held that the standard rule is that a consumer will be considered grossly negligent if he/she follows a link in an email and then hands over personal information.[90] The latter argument is unconvincing in this author's opinion. The Norwegian Supreme Court stated, in 2004, in a case regarding protection of the PIN number for a payment card, that the concept of gross negligence implies exhibiting a significant degree of carelessness.[91] Many serious actors, including public actors and banks in Norway, send emails to consumers requesting that they do precisely what

Act 24 April 2015 on Payment Services, section 62(3). This corresponds to the current rule under the Danish Act 8 June 2017 nb 652 on Payments, section 100(4).

[85] Danish Consumer Dispute resolution for financial services, Decisions 4/2018, 15/2018 and 290/2018.

[86] Danish Consumer Dispute resolution for financial services, Decision 290/2018.

[87] Norwegian Consumer Dispute Resolution for Financial Services, cases FinKN-2018-362, FinNK-2017-649, FinKN-2018-530 and FinKN-2017-506.

[88] Norwegian Consumer Dispute Resolution for Financial Services, case FinKN-2017-649.

[89] As explained in section B.III, in Norway BankID is used for authentication by a range of public and private actors.

[90] Norwegian Consumer Dispute Resolution for Financial Services, case FinKN-2018-311, is an example of a dispute resolution case in which it was concluded that it was not grossly negligent to fall for a phishing attack.

[91] Norwegian Supreme Court case, 19 March 2004, Rt. 2004 s. 499: *'grov uaktsom oppførsel må representere «et markert avvik fra vanlig forsvarlig handlemåte»'*.

Electronic copy available at: https://ssrn.com/abstract=3583369

was requested by the phishing email. As long as serious actors continue to engage in this practice, it seems unfair to conclude that consumers who follow similar instructions in phishing emails are exhibiting a significant degree of carelessness.

The Norwegian Consumer Dispute Resolution body also found that disclosing security information on the phone as part of a vishing scam constitutes gross negligence on the part of the consumer.[92] The cases involved so-called tech-support scams, in which fraudsters called people in a variety of countries and claimed to be tech-support providers from Microsoft.[93] In four similar vishing-scam cases, the Swedish Consumer Dispute Resolution also concluded that the consumers had acted in gross negligence.[94]

Family and friends have easier access to security information than strangers. For example, a consumer may keep a note of his/her PIN number at home or a spouse's password may be guessed because it includes their child's name and age. The question will then be whether this constitutes a grossly negligent breach of the obligations under Article 69 of PSD 2 and the payment services contract. Experience in Norway in cases of familiar fraud suggests that the bar for liability due to gross negligence is also low. In a case from Oslo City Court, a woman was found to have acted in a grossly negligent manner by using her BankID in the same room as her spouse, who suffered from a gambling addiction and who gained access to her password by looking over her shoulder.[95] The Norwegian Consumer Dispute Resolution for Financial Services body has concluded that writing down a BankID password and keeping it at home with the one-time-code device constitutes a grossly negligent breach of obligations, even though the

[92] Norwegian Consumer Dispute Resolution for financial services, cases FinKN-2018-718, FinKN-2018-102, FinKN-2014-526, FinKN-2014-474 and FinKN-2013-496. According to Reinhard Steennot, *Reduced Payer's Liability for Unauthorized Payment Transactions under the Second Payment Services Directive (PSD2)* 34 Computer Law & Security Review 954, 955 (2018), Microsoft vishing scams have also been dealt with by the expert panel of the Belgian Ombudsman for financial services.

[93] According to the Global Tech Support Scam Research 2018, consumers have become more suspicious of potential tech support scams as awareness about such scams has risen in recent years. However, tech-support scams continue to be successful, causing significant loss to those who fall for them. Athima Chansanchai, *Online Scammers Cost Time and Money. Here's How to Fight Back* (15 October 2018), https://news.microsoft.com/on-the-issues/2018/10/15/online-scammers-cost-time-and-money-heres-how-to-fight-back/.

[94] Swedish Consumer Dispute Resolution, decisions 2018-06-14; 2017-07814 (I) and 2017-13660 (II), and Cases 2018-06-14; 2017-10285 (I) and 2017-12130.

[95] Norwegian District Court (Oslo tingrett) Case 20. November 2013, TOSLO-2013-153024.

Electronic copy available at: https://ssrn.com/abstract=3583369

consumer was 92 years old and suffered from Alzheimer's.[96] Because the concept of negligence is vague and depends on an assessment of individual circumstances, it is unsurprising that conclusions differ across cases.[97] Still, Norwegian case law in particular seems to set a very low threshold for concluding that consumers are grossly negligent.

3. The Concept of 'Intent' in Light of Situations of Familiar Fraud

When family or friends gain access to the security information needed to make a payment transaction without the consent of the account owner, the transaction is, according to Article 64 Section 1 of PSD 2, unauthorised. However, if a consumer freely hands over the security information necessary to authenticate as the account holder, the question arises as to whether the consumer has breached his/her obligation to 'keep personalised security credentials safe' under Article 69 of PSD 2 with intent. If so, the consumer is liable for the loss according to Article 74 Section 2 of PSD 2. This is a particularly important question in the context of familiar fraud. The sharing of security information can be practical, if one party is sick or digitally more illiterate than the other, for example. A Norwegian woman gives her BankID security credentials to her husband in order to get help with her tax declaration, for example. The husband then misuses this information to make unauthorised payment transactions.

What should be considered an intentional breach of obligations is not entirely clear and is not further specified in PSD 2 or its recitals. According to the Danish Act on Payments, section

[96] Norwegian Consumer Dispute Resolution on Financial Services, decision FinKN-2014-550. The conclusion and arguments differ from those raised in a case from the British Financial Ombudsman Service, *Case 116/01*, Ombudsman News, Issue 116, 4 (March/April 2014), https://www.financial-ombudsman.org.uk/publications/ombudsman-news/116/issue116.pdf, relating to an elderly woman who kept her credit card with the letter that showed its PIN in the drawer of her nightstand. Her granddaughter stole the card and the PIN and made withdrawals from the account. The bank claimed that the cardholder had acted with gross negligence by keeping the card and PIN together in the drawer. The Financial Ombudsman pointed out that keeping the card and PIN together in a wallet and carrying it in a public place might have constituted gross negligence. However, they maintained that it was reasonable to believe that the nightstand drawer was secure because it was in the cardholder's home. The Financial Ombudsman concluded that the cardholder had not acted with gross negligence.

[97] The British Financial Ombudsman has followed a somewhat divergent path in this area. In some cases, the Ombudsman has concluded that falling for phishing attacks implies grossly negligent actions on the part of the consumer: British Financial Ombudsman, cases DRN2755811 and DRN6823682. However, it has reached the opposite conclusion in a number of cases: British Financial Ombudsman, cases DRN9485561, DRN7602894, DRN4773354 and DRN3853213.

Electronic copy available at: https://ssrn.com/abstract=3583369

100(2), a consumer is liable for the entire loss resulting from an intentional breach of obligations in general. However, section 100(5) of the same Act is more specific and covers the intentional breach of the obligation to keep security credentials safe. According to this section, consumers are only liable for the resulting loss where security credentials were given away with intent *and* the consumer should have understood that this might lead to misuse of the payment instrument.[98] Thus, a consumer who intentionally hands over security credentials will not be liable in situations where he/she could not have understood that this might lead to misuse. There are no decisions relating to the current rule, which transposes PSD 2. However, in a decision from 2008, the Danish Consumer Dispute Resolution body concluded that the consumer was not liable for loss after misuse of a payment card where the cardholder had given her friend access to the card and PIN number.[99] The cardholder did this because she was hospitalised and needed help to withdraw some cash. Her friend misused the card to make several unauthorised transactions. The case was resolved under the Danish rules which existed prior to the implementation of PSD 1.[100]

According to the Swedish Act on Payment Services, chapter 5a, section 3, a consumer is liable for up to SEK 12,000 when a grossly negligent breach of obligations leads to an unauthorised payment transaction. However, if the consumer is considerably to blame (*'[h]ar … handlat särskilt klandervärt'*), he/she is liable for the entire loss. Hence, the wording of the Swedish payment services act is not linked to an intentional breach of obligations, but to the degree of blame. A grossly negligent breach of obligations leads to an individual share of SEK 12,000, while an even more significant degree of carelessness leads to full liability for consumers. In most cases, the breach of obligations with intent will imply that the consumer is considerably to blame. However, this is not necessarily true.

[98] Danish Act 8 June 2017 nb. 652 on Payments, section 100(5): *'Betaleren hæfter uden beløbsbegrænsning for tab, der opstår som følge af andres uberettigede anvendelse af betalingstjenesten, når den til betalingstjenesten hørende personlige sikkerhedsforanstaltning har været anvendt og betalerens udbyder godtgør, at betaleren med forsæt har oplyst den personlige sikkerhedsforanstaltning til den, der har foretaget den uberettigede anvendelse, og at det er sket under omstændigheder, hvor betaleren indså eller burde have indset, at der var risiko for misbrug.'*

[99] Danish Consumer Dispute Resolution for Financial Services, decision 146/2008.

[100] Revoked Danish Act 28 March 2008 nb. 259, section 11(6).

Electronic copy available at: https://ssrn.com/abstract=3583369

The wording of the implementation of Article 74 Section 2 of PSD 2 in Denmark and Sweden differs from that of the directive. However, it makes sense based on the general assumption in Scandinavian tort law, where intention is typically linked to the legally relevant damage, not to a breach of obligations as such.[101] In Norway, the question of whether intent in relation to breach of contract must include not only the breach of contractual obligations, but also ensuing loss has been raised in legal theory circles.[102] It has been argued that an intentional mistake under contract law implies intent in relation to the breach of contract duties *and* negligence related to the consequences of such breach.[103] In Norway, the wording of the Norwegian Financial Contracts Act, section 35, third section, third sentence, implementing the corresponding rule under Article 61 Section 2 of PSD 1, is similar to that in the directive. The Norwegian Consumer Dispute Resolution on Financial Services body seems to base its decisions on an understanding of the rule which implies that intent in relation to breach of the contractual obligation is sufficient for full liability for the consumer.[104] In one decision, an old lady gave her payment card and PIN number to her granddaughter.[105] The old lady had a heart disease and asked the granddaughter for help with grocery shopping. The case is somewhat similar to the Danish case with the hospitalised woman, but with a different result.

IV. Concluding Remarks

As this section shows, the PSD 2 liability regime does provide for important consumer protection in cases of fraud related to payment services. However, the regime also gives rise to important challenges. PSD 2 leaves the concept of intent and gross negligence undefined, leaving it up to national traditions and decision-makers to determine its interpretation on a rather *ad hoc* basis. In particular, the liability regime seems to provide rather limited protection against

[101] Trine-Lise Wilhelmsen and Birgitte Hagland, *Om erstatningsrett Med utgangspunkt I tekster av Peter Lødrup*, 140 (Oslo: Universitetsforlaget 2017). See also Christian Bar and Eric M. Clive, *Principles, Definitions and Model Rules of European Private Law: Draft Common Frame of Reference (DCFR)*, Article VI.3:101 363 (Munich: Sellier European Law Publishers, 2009).

[102] Viggo Hagstrøm, *Obligasjonsrett*, 479 (Oslo: Universitetsforlaget, 2011); Knut Kaasen, *Petroleumskontrakter med kommentarer til NF 05 og NTK 05* (Oslo: Universitetsforlaget, 2006) with further references.

[103] Viggo Hagstrøm, *Obligasjonsrett*, 479 (Oslo: Universitetsforlaget, 2011).

[104] Norwegian Consumer Dispute Resolution on Financial Services, decisions FinKN-2018-272 and FinKN-2016-496.

[105] Norwegian Consumer Dispute Resolution on Financial Services, decision FinKN-2016-496.

Electronic copy available at: https://ssrn.com/abstract=3583369

some of the most common methods of consumer-targeted online financial fraud. The need for legal measures are further explored in section E.

D. Consumer Liability for Familiar Fraud Related to Credit Contracts

I. Introduction

When rules on liability for unauthorised payment transactions were first introduced in PSD 1, there was in practice little digitalisation of financial services other than payment services. The digitalisation of financial services has expanded enormously over the past decade. Today, numerous financial services are available online and can be accessed through the use of technologies that enable authentication and electronic signatures. Hence, the risk of fraud has increased in this area and is no longer limited to unauthorised payment transactions. Financial services related to credit products are particularly vulnerable to fraud due to the potential monetary gains. The experience in Scandinavian countries shows that full digitalisation of credit agreements has led to extensive fraud-related problems. The methods that can be used to commit fraud related to digital credit contracts are in theory the same as those used to make unauthorised payment transactions. A phishing attack could, for example, be used to commit identity theft, in which a credit agreement is then signed in the victim's name. However, when applying for a loan, one needs to provide additional personal information as part of the credit assessment process. This might explain why case law from the Scandinavian countries indicates that familiar fraud is the most common method of fraud related to credit agreements. Examples include situations in which the fraudster is a family member, the victim's employer, a social worker or a drug dealer committing identity theft in order to fraudulently execute credit agreements.

For unauthorised payment transactions, the loss originally accrues to the customer. According to the rules analysed above, the liability regime based on PSD 2 allocates this loss to the payment service provider on certain conditions. In cases of fraudulent execution of credit agreements, the loss originally accrues to the creditor, because the credit amount is paid to the fraudster, who does not pay it back. The question addressed in this section is to what extent there are legal grounds for the creditor to allocate this loss to the victim.[106] This question is not

[106] The fraudster will, of course, be liable to both the financial institution and the victim of identity theft. As explained in the introduction, this paper focuses on liability issues between financial institutions and fraud-victims.

Electronic copy available at: https://ssrn.com/abstract=3583369

addressed by European law. In this section, case law from Norway, Sweden and Denmark will be used as examples. In all Scandinavian countries, the liability regime for identity-theft-related crime depends on general rules of contract and tort law. For the most part, these rules are similar across the Scandinavian countries.[107] The relevant case law includes examples of consumer liability based on contract law (section D.II), liability based on principles of unjust enrichment (section D.III) and liability based on general rules of tort (D.IV). But first, some comments will be made on the relationship between the rules on payment services fraud and credit contract fraud.

If the credit amount is paid directly from the creditor to an account held by the fraudster, there is no unauthorised payment transaction. Hence, the PSD 2 liability regime does not apply. However, credit-agreement fraud may also involve payment transactions covered by PSD 2. First, in certain situations, PSD 2 covers credit linked to the issuance of a credit card.[108] Unauthorised transactions from a credit card account will normally fall under the PSD 2 liability regime. The regime applies even if the credit card agreement as such is void because it is based on identity theft.[109] The typical situation is that of a fraudster who, through the misuse of a general identification scheme, obtains a credit card in the victim's name and then makes a transaction from this credit account. The conclusion that PSD 2 covers these situations is, however, somewhat uncertain. The liability regime seems to be based on the assumption that the unauthorised transaction relates to a valid payment services contract. Customer liability is linked to whether the customer fulfilled the obligations under Article 69 of PSD 2, which refers to contract terms. If the underlying agreement for payment services related to the issuance of the credit card is based on identity theft and hence a fake electronic signature, it makes little

[107] Christina Ramberg, *The Hidden Secrets of Scandinavian Contract Law*, 50 Scandinavian Studies in Law 250 (2010); Kåre Lilleholt, *Application of General Principles in Private Law in the Nordic Countries*, XX Juridica International Law Review University of Tartu (2013); Trine-Lise Wilhelmsen and Birgitte Hagland, *Om erstatningsrett Med utgangspunkt I tekster av Peter Lødrup*, 38 (Oslo: Universitetsforlaget, 2017).

[108] Article 18(4) and Recital 40, PSD 2.

[109] Case C-295/18 *Mediterranean Shipping Company (Portugal) — Agentes de Navegação SA vs Banco Comercial Português SA, Caixa Geral de Depósitos SA* (11 April 2019) relates to a similar question, namely whether the scope of PSD 1 'includes the execution of a direct-debit payment order issued by a third-party on an account which it does not hold, where the holder of that account has not entered into a payment service contract for a single transaction, or a framework contract for the provision of payment services with that credit institution'. Based on a teleological interpretation, the ECJ concluded that the directive was applicable.

Electronic copy available at: https://ssrn.com/abstract=3583369

sense to ask whether the customer has fulfilled his or her contractual obligations. However, transactions based on a fraudulently executed credit card agreement are definitely made without the victim's consent and the victim will be in need of the protection provided by the directive.[110]

Second, if the credit amount is paid to an account owned by the victim and then transferred to the fraudster, the PSD 2 liability regime will apply in relation to the payment service provider. However, the creditor will often be a different financial institution. By the time the fraud is detected, it may be too late to reclaim the amount from the payment service provider. It will also be an additional burden on the consumer to handle two disputes at the same time: one against the payment service provider based on an unauthorised payment transaction and one against the creditor.

II. Liability Based on Contract Law

When a contract is concluded fraudulently based on identity theft, the contract will typically be void. When the fraudster creates a fake electronic signature in the victim's name, the victim of course does not intend to enter into a legally binding relationship.[111] Such intent is normally needed in order to establish a binding agreement. However, rules on the burden of proof can make it difficult for the victim to prove that the credit agreement was in fact signed by a fraudster. In a 2017 case, the Swedish Supreme Court decided that when the creditor can prove that the credit agreement was signed using what is defined as an advanced electronic signature under the eIDAS Regulation, the contract will bind the parties unless the consumer can provide proof that it is probable someone else created the electronic signature.[112] Such proofs can of course be difficult to establish. In the Supreme Court case, the consumer failed to provide the

[110] Another important practical aspect related to this kind of fraud is the lack of a contract law relationship. This could bar the dispute from being settled in alternative dispute resolution. For example, the Norwegian Dispute Resolution for Financial Services only takes into consideration disputes based on a contract law relationship. For that reason, cases in which a credit card agreement has been executed based on identity theft are dismissed. See Norwegian Consumer Dispute Resolution, decisions FinKN-2013-422 and FinKN-2017-279.

[111] In such situations, the terms for concluding a binding agreement will not be complied with. See Norwegian Act 31 May 1918 nb. 4 on Contracts (Norwegian Contracts Act), chapter 1; Swedish Act 11 June 1915 nb. 218 on Contracts (Swedish Contracts Act), chapter 1; and Danish Act on Contracts and Other Juristic Acts pertaining to Property, Consolidation Act No. 600 of 8 September 1986 (Danish Contracts Act), chapter 1.

[112] Swedish Supreme Court case NJA 2017, s. 1105 *«Det har ansetts att långivaren måste visa att det är den påstådda avancerade elektroniska underskriften som har använts. Om så sker måste innehavaren av underskriften göra antagligt att användandet av underskriften skett obehörigen.»*

Electronic copy available at: https://ssrn.com/abstract=3583369

necessary proof that she had not created the electronic signature herself. However, if consumers can prove that they did not provide the electronic signature or did not give consent for someone else to create the signature on their behalf, case law in Sweden and Norway would seem to indicate that the credit contract will not be binding under contract law. This is true even when the victim has freely disclosed their BankID information to, for example, family members.[113]

The Danish Supreme Court has taken a different position on the question of binding contracts. In January 2019, the court found in two cases on the same day that victims of identity theft are bound on contract law grounds to credit agreements concluded by others in their name.[114] In the first case, a young man gave the key and password to his NemID to a drug dealer as a means of paying a drug debt of DKK15,000. According to the man's explanation, he felt threatened by the drug dealer to hand over his NemID security information. The drug dealer then used this information to conclude a credit agreement in the victim's name. As part of the credit rating process, the fraudster sent falsified documents to the creditor, including fake salary slips in the name of the victim. The credit amount was paid to the victim's account, to which the fraudster had access because of the identity theft, and then transferred to an account held by the fraudster. The other case concerned a young man who felt threatened to disclose his NemID information to two acquaintances. According to the man's explanation, the two perpetrators threatened him with violence and subsequently used his NemID information to conclude a credit agreement. The day after, the young man reported the crime to the police. In both cases, the question for the Supreme Court was whether the victim was bound by the credit agreement contract.

In both cases, the Supreme Court found evidence that the credit agreement was not in fact concluded by the victims. Still, the court found in both cases that the victims were bound by the credit agreement. The court's reasoning is very limited and difficult to understand. The Supreme Court stated that the victims had acted negligently by handing over their NemID information and by failing to report this to the bank afterwards. Although the Danish Supreme Court did not explicitly state the basis for its decision, it seems to be based on a version of the concept of apparent representation. According to rules on representation, a principal may grant

[113] Swedish Appeal Court (Svea Hovrätt) Case 19 June 2018 T 11184-17 and Norwegian Appeal Court (Borgarting lagmannsrett) Case 13 March 2017 LB-2016-43622.

[114] Danish Supreme Court, Cases 82/2018 8 January 2019 *A vs. Basisbank A/S* and 87/2018 8 January 2019, *B vs. Basisbank A/S*.

Electronic copy available at: https://ssrn.com/abstract=3583369

authority to a representative to act on behalf of the principal. The concept of so-called apparent representation is acknowledged under contract law in the Scandinavian countries.[115] This concept implies that if a person causes a third party, reasonably and in good faith, to believe that the person has authorised a representative to perform certain acts, the person is treated as a principal who has so authorised the apparent representative. This type of authority is called 'apparent' because it is based on the appearance of things. In Article II.-6:103, third paragraph, of the Draft Common Frame of Reference (DCFR), the principle is described as follows: 'If a person causes a third party reasonably and in good faith to believe that the person has authorised a representative to perform certain acts, the person is treated as a principal who has so authorised the apparent representative.'[116]

The grounds for apparent representation could be negligent actions on the part of the principal.[117] In my opinion, the reasoning of the Danish Supreme Court is flawed. In both cases, the victim had invoked threats as grounds for invalidity, but the Supreme Court failed to acknowledge this. For the purpose of this article, however, it is unnecessary to further discuss the Supreme Court's reasoning. Regardless of whether one agrees with the Supreme Court, the cases clearly exemplify consumer liability based on contract law in situations of identity theft related to credit agreements.

III. Liability Based on Principles of Condictio Indebiti *(Unjustified Enrichment)*

In situations in which the credit amount has been paid to an account held by the identity theft victim and immediately transferred to the fraudster's account, the victim could under certain circumstances be held responsible against the creditor under the principle of *condictio indebiti*. In the Scandinavian countries, this principle constitutes an independent regime pertaining to the restitution of mistaken payments.[118] An assessment is made in the individual case as to whether

[115] Kåre Lilleholt, *Kontraktsrett og obligasjonsrett*, 70 (Oslo: Cappelen Damm Akademisk, 2017); Kurt Grönfors, *Ställningsfullmakt och bulvanskap* (Stockholm: Norstedt, 1961); and Lennart Lynge Andersen, *Aftaleloven med kommentarer*, 6th ed., 349-366 (Copenhagen: Jurist- og Økonomiforbundets Forlag, 2014).

[116] Christian Bar and Eric M. Clive, *Principles, Definitions and Model Rules of European Private Law: Draft Common Frame of Reference (DCFR)*, 443 (Munich: Sellier European Law Publishers, 2009).

[117] Henrik Udsen, *Uagtsomhed som aftalestiftende retsfaktum – et bidrag til den aftaleretlige forpligtelseslære* 119 Tidsskrift for Rettsvitenskap 104 (2006).

[118] On the principle of *condictio indebiti*, see, with further references: Kåre Lilleholt, *Kontraktsrett og obligasjonsrett*, 484 (Oslo: Cappelen Damm Akademisk, 2017); Torsten Iversen, *Obligationsret på grundlag af Bernhard Gomards obligationsret* 3. del, 236 (Copenhagen: Jurist- og økonomiforbundets forlag, 2018);

Electronic copy available at: https://ssrn.com/abstract=3583369

the payment should be restituted. The assessment is made with respect to the good faith of the recipient, possible negligence of either party and other factors.

Especially in Sweden, rules on *condictio indebiti* have been invoked by the creditor to constitute legal grounds for repayment by the identity theft victim.[119] A case from the Swedish Appeal Court relates to a situation of family fraud.[120] An elderly father received help from his son to learn how to pay his bills on the internet. While helping his father, the son got access to his father's BankID information. The son misused this information to enter into 16 different credit agreements in his father's name. When the credit amount was paid to the account of the father, the son immediately transferred the money to his own account. When the father found out about the son's actions, he reported him to the police. The father was not found to be contractually bound by the credit agreements made in his name by his son. However, both the District Court and the Appeal Court found that he was obligated to repay the credit amount to the creditor based on the principle of *condictio indebiti*. Central to the arguments of the Appeal Court is that the father acted negligently by making it possible for the son to gain access to his BankID.

IV. Liability Based on the Law of Tort

A loss accrues to the creditor when the credit amount is disbursed and the identity theft victim and the fraudster fail to repay according to the credit agreement. According to general rules on tort, applied in all Scandinavian countries, a person can be held liable for such loss if it results from his or her negligent action.[121] As explained, the consumer typically enables the resulting fraud by making security mistakes. For example, a consumer clicks a link in a phishing email and hands over his or her security information, despite warnings not to do so, or fails to keep an electronic banking password safe from his or her partner. The question is whether this

---

Norwegian Supreme Court Case 9 March 1985 Rt. 1985 s. 290; Mårten Schultz, *Nya argumentationslinjer i förmögenhetsrätten,* Svensk Juristtidning 946 (2009).

[119] See for example Swedish District Court (Stockholms tingsrätt) Case 8 June 2018, T 8297-17; Swedish District Court (Attunda Tingsrätt) Case 10 May 2019, T 5632-18; and Swedish District Court (Södertörns tingsrätt) Case 23 May 2019, T 12442-18.

[120] Swedish Appeal Court (Svea Hovrätt) Case 30 November 2017, T 2412-17.

[121] Trine-Lise Wilhelmsen and Birgitte Hagland, *Om erstatningsrett Med utgangspunkt I tekster av Peter* Lødrup, 87 (Oslo: Universitetsforlaget, 2017); Håkan Anderson, *Ansvarsproblem i skadeståndsrätten Skadeståndsrättsliga utvecklingslinjer Bok 1*, 61 (Uppsala: Iustus Förlag, 2013); and Torsten Iversen, *Obligationsret på grundlag af Bernhard Gomards obligationsret* 3. del, 208 (Copenhagen: Jurist- og økonomiforbundets forlag, 2018).

Electronic copy available at: https://ssrn.com/abstract=3583369

implies negligent action resulting in liability under tort. In contrast to the regulation of unauthorised payment transactions, gross negligence is not required in order to make the victim liable under general rules on tort.

In Norway, in particular, there is plenty of case law from the district courts and the courts of appeal on this matter.[122] There are, however, no cases from the Supreme Court, which might explain why case law from the lower courts seems very inconsistent. In a number of cases, the identity theft victim has been found to be responsible to the creditor.[123] Several cases relate to situations in which a person entered into credit agreements in his or her spouse's name. The bar for constituting liability is in some cases extremely low. In one case, a woman was found to have acted negligently because she was typing her BankID password while sitting next to her spouse on the sofa, making it possible for him to see the password.[124] In a similar case. a husband received a prison sentence for identity theft and fraud after misusing his wife's BankID to enter into a number of credit agreements in her name.[125] Reclaiming such sums from a person in prison is difficult, so the bank sued the wife in a civil law case. The wife was held responsible because she used a password that was easy for her husband to guess. The wife claimed that the fraud was enabled by the bank's poor security measures. For example, the credit amount was paid directly to the husband's account. However, the court found that the wife was responsible for the total amount of the credit, approximately NOK1,000,000 (EUR 100,000), under the rules on tort.

[122] Norwegian Appeal Court (Borgarting lagmannsrett) Case 6 October 2014, LB-2014-13514; Norwegian Appeal Court (Borgarting lagmannsrett) Case 13 March 2017, LB-2016-43622; Norwegian District Court (Øvre Romerike tingrett) Case 27 February 18-148976TVI-OVRO; Norwegian District Court (Øvre Romerike tingrett) Case 22 February 2018 17-098711TVI-OVRO; Norwegian District Court (Øvre Romerike tingrett) Case 26 November 2018 18-127575TVI-OVRO; Norwegian District Court (Follo tingrett) Case 21 March 2018 17-169552TVI-FOLL; and Norwegian District Court (Gjøvik tingrett) Case 1 February 2018 15-168226TVI.

[123] Norwegian Appeal Court (Borgarting lagmannsrett) Case 6 October 2014 LB-2014-13514; Norwegian Appeal Court (Borgarting lagmannsrett) Case 13 March 2017 LB-2016-43622; Norwegian District Court (Øvre Romerike tingrett) Case 27 February 18-148976TVI-OVRO; Norwegian District Court (Øvre Romerike tingrett) Case 22 February 2018 17-098711TVI-OVRO; Norwegian District Court (Øvre Romerike tingrett) Case 26 November 2018 18-127575TVI-OVRO; Norwegian District Court (Follo tingrett) Case 21 March 2018 17-169552TVI-FOLL; and Norwegian District Court (Gjøvik tingrett) Case 1 February 2018 15-168226TVI.

[124] Norwegian District Court (Haugaland tingrett), Case 13 June 2018 17-197796TVI-HAUG.

[125] Norwegian Oslo City Court (Oslo tingrett), Case 23 October 2018 18-074832TVI-OTIR/01.

Electronic copy available at: https://ssrn.com/abstract=3583369

In a case from the Norwegian Consumer Dispute Resolution for Financial Services, an elderly woman suffering from Alzheimer's had written down her BankID password and kept it together with her code device at home.[126] The bank was informed that the woman had a supporting guardian and hence was unable to manage her finances without help. A friend of her son misused the woman's BankID information to enter into a credit agreement in her name. The Consumer Dispute Resolution for Financial Services concluded that the woman had acted with gross negligence by writing her password down. According to the Consumer Dispute Resolution, there was no reason to criticise the bank for not contacting the guardian, because the loan was granted based on an automatic process. In yet another case from the Appeal Court, a young woman was held responsible for credit taken out in her name by her mother, who was suffering from a gambling addiction.[127] The relevant case law also includes some decisions concluding that the consumer was not liable.[128]

From a theoretical perspective, the arguments in most of the cases which concluded that the victim was liable are in my opinion seriously flawed. Consumers are held to unreasonably high standards in order to avoid liability. It is considered grossly negligent to write down a BankID password, even when suffering from Alzheimer's, and negligent to use an electronic bank account when sitting on a sofa beside your spouse. The financial institutions are held liable to correspondingly low standards. All cases show a lack discussion of consumer protection issues and the significance of arguments related to the financial institution's opportunities to avoid loss through security measures and the ability to distribute the costs generated by fraud. However, the point in relation to the research question in this paper is to show that Norwegian courts in practice allocates losses as a result of fraudulently concluded credit agreements from financial institutions to the fraud victims under general rules on tort.

V. Concluding Remarks

In this section, consumer liability for fraud in the conclusion of credit agreements has been discussed. There is no specific regulation of these issues in national law in the Scandinavian

[126] Norwegian Consumer Dispute Resolution for Financial Services, Case FinKN-2014-550.

[127] Norwegian Appeal Court (Frostating lagmannsrett) Case 31 January 2019 18-039633ASD-FROS.

[128] Norwegian Appeal Court (Agder lagmannsrett), Case 3 April 2017 LA-2017-135340; Norwegian District Court (Nedre Telemark tingrett), Case 3 November 2016 16-054343TVI-NETE; Norwegian District Court (Follo tingrett) Case 11 June 2015 14-193249TVI-FOLL; and Norwegian District Court (Gjøvik tingrett), Case 16 April 2018 17-170313TVI-GJOV.

Electronic copy available at: https://ssrn.com/abstract=3583369

countries. And practices diverge as to how general rules on contract and tort should be applied when a general authentication scheme has been misused by a fraudster to sign a credit agreement in another's name. However, in all Scandinavian countries, the consumer will often be held liable if security information has been handled in a negligent way.

E. Who Should Pay When Things Go Wrong?

This paper has provided some insight into how losses resulting from online financial fraud are allocated between the consumer and the financial services provider in the Scandinavian countries. In many situations, consumers are left to deal with the losses caused by such fraud, including losses related to authorised push payment scams, phishing attacks and identity theft in credit contracts. The aim of the liability regime for unauthorised payment transactions under PSD 2 is to allocate losses in a way that enhances trust in the system and incentivises payment service providers to develop and use high-security solutions for electronic payments.[129] At a more general level, the European Commission has, as explained, emphasised that the Digital Single Market 'should offer EU citizens the same level of safety and the same expectations in online dealings that they have in their day-to-day offline life'.[130] The practices described in this paper make it evident that we are not there yet. Financial-services fraud exists in the offline world as well. However, it was more difficult, for example, to sign a credit agreement in another person's name when such agreements had to be signed physically at the office of the local bank branch. And if someone still managed to pull off fraud in this environment, the victim was unlikely to be held responsible.

Hence, the digitalisation of the financial services industry has in practice led to a shift in who bears the risk for attacks on financial institutions. As explained above, humans are often the weakest links in the security chain, enabling fraudsters to target consumers instead of financial institutions directly. The result of digitalisation then is that consumers are made to carry a far greater part of the inherent risk of fraud. As David Mitchell rhetorically put it:

[129] Recital 7, PSD 2.

[130] European Commission, Commission Staff Working Document, A Digital Single Market Strategy for Europe - Analysis and Evidence Accompanying the document Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A Digital Single Market Strategy for Europe, SWD (2015)100 final, 51 (6 May 2015).

Electronic copy available at: https://ssrn.com/abstract=3583369

> With the concept of 'identity theft', however, banks try to absolve themselves of that fundamental responsibility. So now if someone steals from them in disguise, they claim that's an issue between the thief and the person the thief is disguised as. If a gang of armed bank robbers were wearing Tony Blair masks, would the bank now debit all the stolen cash from the former prime minister's account?[131]

For individual victims, the consequences can be severe. However, the situation is not ideal for financial services providers either, because the situation might result in decreased trust in the digital financial market as such. Because protection against the consequences of cybersecurity fraud is a political priority in the EU,[132] the conclusion must be that enhanced consumer protection is necessary in this area. A range of measures have already been implemented in order to meet challenges relating to protection from online financial fraud, including a proposal for a directive on combating fraud and counterfeit (non-cash) means of payment;[133] a proposal for an EU cybersecurity agency; and an EU framework for cybersecurity certification.[134] Such preventive measures are important, but they will hardly eliminate cybersecurity fraud. This is why the question of the ex post regulation of liability and the choice of loss allocation is important. In particular, this paper raises the question of whether a more significant portion of the liability following unauthorised payment transactions should be allocated to payment service providers.

Regarding authorised push payment scams, the discussion in section C.III.1 shows that consumers are left with liability when they are victims of such scams. Such scams can be just as sophisticated as phishing attacks, and the need for consumer protection seems to be the same. The problem is partly a result of the system under PSD 2, where a payment order is deemed to have been executed correctly, and hence authorised, even in situations where the name of the

---

[131] David Mitchell, *"Identity Theft"? It's Daylight Robbery by the Banks*, The Guardian (25 November 2018) https://www.theguardian.com/commentisfree/2018/nov/25/identity-theft-is-daylight-robbery-banks.

[132] See section B.I.

[133] See Proposal for a Directive of the European Parliament and of the Council on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA, COM(2017) 489 final 2017/0226 (COD) Brussels 13.9.2017.

[134] European Commission, *Cybersecurity - An EU Cybersecurity Agency and an EU Framework for Cybersecurity Certification* (19 September 2017), https://ec.europa.eu/digital-single-market/en/news/cybersecurity-eu-cybersecurity-agency-and-eu-framework-cybersecurity-certification.

Electronic copy available at: https://ssrn.com/abstract=3583369

payee provided by the payer does not corresponds to the owner of the account to which the money is transferred. As security expert Peter Hamilton put it:

> The Payment Systems Regulator, which has the duty of enforcing the regulations, should act to make all banks carry out proper checks to ensure consistency in all the information at the bank's disposal. Relying just on the account number and sort code is not good enough, particularly because this kind of fraud is now so common.[135]

As long as the existing liability regime forces customers to bear the entirety of the risk of authorised push payment scams, there will be few incentives for payment service providers to implement security measures designed to prevent such scams.

Further, the existing PSD 2 regulation relies heavily on an undefined concept of gross negligence and intent, which leads to divergent practices. The divergent results in cases dealing with phishing attacks exemplify the consequences of the liability regulation's lack of clarity.[136] In Norway and Sweden in particular, falling for sophisticated phishing attacks is viewed as gross negligence on the part of the consumer. In order to ensure a coherent interpretation of the directive, and a sufficient level of consumer protection, clarification of the rules is required. However, in Scandinavian countries an important protection remains in the fact that lawmakers have decided to limit consumer responsibility to NOK/SEK12,000 and DKK 8000 (approximately EUR 1,000–1200) in cases involving a grossly negligent breach of obligations. In my opinion, the European regulator should consider making this a general rule, applicable in all Member states.

Despite these weaknesses in the regulation of payment services, consumers are fairly well protected against fraud related to payment transactions, at least in the Scandinavian countries. The main problem with the European regulation seems to be the absence of regulation of liability issues resulting from fraud in financial services other than payment services. This paper has discussed how losses resulting from credit agreement fraud are allocated according to general rules on contract and tort in the Scandinavian countries. In these countries, the result is

[135] Peter Hamilton, *Who Is Liable for Online Banking Scams?* (3 July 2017) https://www.moneymarketing.co.uk/issues/29-june-2017/peter-hamilton-liable-online-banking-scams/.

[136] Nicole S van der Meulen, *You've Been Warned: Consumer Liability in Internet Banking Fraud*, 29 Computer Law & Security Review 713 (2013) describes the same divergent practices in relation to phishing in Germany.

Electronic copy available at: https://ssrn.com/abstract=3583369

dramatic inconsistencies in how liability questions are dealt with in cases of unauthorised payment transactions on the one hand, and in cases of unauthorised transactions related to other financial services on the other.

In Norway, for example, if BankID is misused to log in to someone else's online account and transfer NOK1,000,000 to the fraudster's account, the payment service provider is liable to repay the amount under to the liability regime for unauthorised payment transactions. Even if the victim has handled the BankID security information in a grossly negligent way, the consumer's liability is limited to NOK12,000. In contrast, if the same BankID device is misused to enter into a credit contract amounting to NOK1,000,000, the victim is to the credit provider for the entire amount, even when only ordinary negligence applies. Hence, losses related to unauthorised payment transactions are allocated from the customer to the financial services provider under the rules in PSD 2, whereas losses related to the execution of a credit agreement are borne by the consumer under national rules on tort.

The risk of fraud is also evident in relation to financial services other than those addressed by this paper. We can easily imagine unauthorised transactions in cryptocurrency, for example, which fall outside the scope of PSD 2, or unauthorised investment transactions. For consumers who have placed their savings in financial instruments, an unauthorised investment transaction could be just as devastating as an unauthorised payment transaction. It is difficult to find a justification for the differences in treatment of unauthorised payment transactions and unauthorised transactions related to other financial services. This is why the Ministry of Justice and Public Security in Norway has requested comments on a proposal that will extend the scope of the PSD 2 liability regime to unauthorised transactions in all types of financial services.[137] The proposal must be understood in light of the practices described above, in which a large number of consumers experience identity-theft-related crime particularly in relation to credit contracts and the fact that the courts' application of the general rules on tort has been very unfriendly to consumers. Even if the proposal must be understood against this backdrop, it raises the question of whether European regulators should adopt a similar proposal.

[137] Norwegian Ministry of Justice and Public Security, *Høring - ny finansavtalelov* (7 September 2017) https://www.regjeringen.no/no/dokumenter/horing---revisjon-av-finansavtaleloven/id2569865/. The author of this paper was employed at the Norwegian Ministry of Justice and Public Security from 2016 to 2017, and worked on the proposal during this time.

Electronic copy available at: https://ssrn.com/abstract=3583369

The financial industry has opposed the proposal in their response to the official hearing. Representing 240 companies, Finance Norway, the central organisation for the financial industry in Norway, has demanded that the liability rule be omitted from the proposal.[138] In their response, they argue that the proposed regulation will create a new, unjustified distinction between financial service providers and providers of other goods and services.[139] They also argue that the proposal will introduce a great risk for financial institutions because there are no limits to their potential responsibility.[140] Under PSD 2, the payment service providers' liability will be limited to the debit or credit amount available on the account. If the same liability regime is applied to credit-agreement fraud, for example, the potential responsibility for financial institutions will be unlimited. Finance Norway also argues that a shift in liability from consumers to financial institutions will lead to increased crime against banks.[141]

The arguments of Finance Norway are indeed valid. However, in my opinion, they do not outweigh the arguments in favour of the proposed rule. The argument related to the unlimited risk inherent in the proposal is particularly interesting. It is true that, in practice, the risk is unlimited when it relates to credit agreements. However, this is true not only for financial institutions but also for consumers. The current system implies that getting a BankID exposes consumers to unlimited risk of loss. This risk goes far beyond life savings. When someone's BankID information falls into the hands of a fraudster, the result could be millions in debt to financial institutions. As explained above, BankID is used by all the country's banks, by public authorities and by an increasing number of businesses in a wide range of sectors. Not having a BankID is not a practical option.

---

[138] Finans Norway, *Høringsuttalelse ny finansavtalelov*, 62 (15 December 2017) https://www.regjeringen.no/no/dokumenter/horing---revisjon-av-finansavtaleloven/id2569865/?uid=af7f501c-5781-4635-b9b4-1f72c4a14fa4.

[139] Finans Norway, *Høringsuttalelse ny finansavtalelov*, 62 (15 December 2017) https://www.regjeringen.no/no/dokumenter/horing---revisjon-av-finansavtaleloven/id2569865/?uid=af7f501c-5781-4635-b9b4-1f72c4a14fa4.

[140] Finans Norway, *Høringsuttalelse ny finansavtalelov*, 62 (15 December 2017) https://www.regjeringen.no/no/dokumenter/horing---revisjon-av-finansavtaleloven/id2569865/?uid=af7f501c-5781-4635-b9b4-1f72c4a14fa4.

[141] Finans Norway, *Høringsuttalelse ny finansavtalelov*, 63 (15 December 2017) https://www.regjeringen.no/no/dokumenter/horing---revisjon-av-finansavtaleloven/id2569865/?uid=af7f501c-5781-4635-b9b4-1f72c4a14fa4.

Electronic copy available at: https://ssrn.com/abstract=3583369

Finance Norway points out that if financial service providers are held responsible for the misuse of BankID in relation to financial services other than payment services, this will lead financial service providers to stop using digital solutions for signing and revert to manual signatures. This is an interesting argument, because the risk of loss already exists and follows from the heightened possibility of fraud resulting from contemporary technical solutions. If these solutions are so unsecure that financial institutions will not use them if forced to deal with the consequences of fraud, then the only reason consumers accept this risk is that they lack alternatives or do not understand the risk they currently assume.[142]

The traditional goal of loss allocation rules is to place the loss on the party who has the greatest power to prevent the loss at the least cost. There is growing evidence that consumers have limited ability to avoid online financial fraud, which is becoming increasingly sophisticated.[143] As Mason and Bohm put it: 'The banks must put more robust methods in place to provide for the security of customers' accounts. They will not do so without the necessary incentive; and while they can pass the loss to their customers, they lack that incentive.'[144] This is true not only for bank accounts but also for processes in other financial services, including trading in financial instruments and credit agreement processes.

A potential consequence of placing the risk on consumers is a loss of trust. Cases of customer liability related to the misuse of BankID or NemID have received wide publicity in all the

[142] On the risks of the BankID system, see Yngve Espelid, Lars-Helge Netland, Andre N. Klinsheim and Kjell J. Hole, *Robbing Banks with Their Own Software—an Exploit Against Norwegian Online Banks*, in Jajodia S., Samarati P., Cimato S. (eds) *Proceedings of the IFIP TC 11 23rd International Information Security Conference* 64 (IFIPAICT vol 278, Springer 2008); Kristian Gjøsteen, *Weaknesses in BankID, a PKI-Substitute Deployed by Norwegian Banks*, in Mjølsnes S.F., Mauw S., Katsikas S.K. (eds) *Public Key Infrastructure. EuroPKI 2008*, vol 5057, 196 (Berlin: Springer, 2008); Jonny Rein Eriksen, *Det er en sikkerhetssvakhet i BankID* (22 March 2019), https://www.digi.no/artikler/kommentar-det-er-en-sikkerhetssvakhet-i-bankid/460792.

[143] Stephen Mason and Nicholas Bohm, *Banking and Fraud* 33 Computer Law & Security Review 237 (2017).

[144] Stephen Mason and Nicholas Bohm, *Banking and Fraud* 33 Computer Law & Security Review 237 (2017). The same point is also made by Schneier, arguing that banks must be responsible for all fraudulent transactions: Bruce Schneier, *Solving Identity Theft* (January 2007), https://www.schneier.com/essays/archives/2007/01/solving_identity_the.html.

Electronic copy available at: https://ssrn.com/abstract=3583369

Scandinavian countries.[145] Falling victim to cybercrime and being exposed to cybercrime in the media can reduce customers' participation in online banking.[146]

Regardless of economic concerns, arguments of fairness are important. What is evident from the Scandinavian case law is that vulnerable consumers with low levels of digital competence are especially exposed to cyberfraud. This is particularly true in countries with highly developed digital solutions for financial services. In the Scandinavian countries, it is very difficult to handle one's personal finances without using online solutions. Most physical bank branches are closed, and those that remain have high charges for manual payment transactions. The financial industry and digitally literate consumers benefit from this development and from digitalisation more broadly, but vulnerable consumers are clearly worse off. Many of the cases described in this paper concern the elderly, the sick, and those who for other reasons need help handling their finances in a digital world. The current rules on liability provide these persons with very limited protection.

Allocating a greater portion of losses to financial institutions could reduce the frequency of online financial fraud, provide some compensation for its victims and distribute the cost of fraud more effectively among those who benefit from financial services.[147] It would also urge financial institutions to develop more secure solutions, without the need for regulators to decide precisely what institutions should do in this respect. Based on these arguments, it is my opinion that the European lawmakers should take a coordinated approach to the regulation of liability and loss allocation, where larger parts of loss after online financial fraud should be allocated from consumers to financial institutions.

---

[145] Kjetil Mæland, *Stjal BankID og lånte 800.000 kroner: Nå må ekskona betale tilbake* (2 November 2018) http://nettavisen.no/artikkel/3423553830; Kjetil Mæland, *BankID-svindel: – Min ektemann misbrukte BankID og tok sitt eget liv* (13 November 2018), https://www.nordlys.no/krim/bankid/svindel/bankid-svindel-min-ektemann-misbrukte-bankid-og-tok-sitt-eget-liv/s/5-34-1002059; Silje Helgesen, *Grovt bedrageri: Kaja (33) ble svindlet av eksen for nærmere en million kroner - KK* (11 May 2019), http://www.kk.no/a/71011523; Karin Lindström, *Jurister varnar: tjänster missbrukar mobilt bank-id* (27 November 2017), https://computersweden.idg.se/2.2683/1.693238/e-id-varning.

[146] Rainer Böhme and Tyler Moore, *How Do Consumers React to Cybercrime?* in *Proceedings of the 7th APWG eCrime Researchers Summit* (2012); Nicole S van der Meulen, *You've Been Warned: Consumer Liability in Internet Banking Fraud* 29 Computer Law & Security Review 713 (2013).

[147] Jeff Sovern, *The Jewel of Their Souls: Preventing Identity Theft Through Loss Allocation Rules*, SSRN Scholarly Paper ID 1342692, 354 (2009), https://papers.ssrn.com/abstract=1342692.

Electronic copy available at: https://ssrn.com/abstract=3583369

Until then: Consumers foot the bill when things go wrong – oftentimes.

Electronic copy available at: https://ssrn.com/abstract=3583369