08.05.2024

Director-General Mr. John Berrigan, DG Fisma

(A copy of this letter will also be sent to Head of Cabinet Mr. Michael Hager, Cabinet of Executive Vice-President Valdis Dombrovskis)

Nordic experiences on the fight against fraud

Dear Mr. Berrigan

With reference to and in appreciation of the meeting between yourself and the Nordic banking associations on April 9 we would like to take the opportunity to follow up on one highly topical matter discussed during the meeting that deserves further elaboration.

The Nordic economies are highly digitalised. There are many advantages to this, such as reduced transaction costs, more informed decision making, and, not least, new, and improved financial services for customers. Furthermore, the risk for physical bank robberies and cash-in-transit robberies has decreased significantly.[1]

However, we are now experiencing new types of digital fraud throughout the region. We are especially worried by fraud performed through **social engineering methods,** i.e., manipulating the consumer to execute the fraud themselves**.** This is a serious societal problem that has grown over the past years. The Nordic community is addressing this issue with urgency, and we support the European Commission's objective to counteract (online) scams. A broad range of measures is needed; we need monitoring and facilitation of information sharing in combination with information campaigns.

With this letter, we would like to share our experience of this kind of fraud. We also outline our thoughts on the existing legislative proposals and point at preventive measures, which are needed to effectively tackle the problem.

The benefits and costs of financial digitalisation
The general European trend is moving towards instant payments, a move that the Nordic region made several years ago. In the Nordics, a vast majority of banking customers have an e-ID and perform their financial services via electronic banking services. In addition, there are now many different payments service providers, and access to data has been opened up. These developments will continue through the Payment Services Directive/Regulation (PSD3/PSR), the Financial Data Access Regulation (FIDA) and the Instant Payments Regulation (IPR).

New services and products are not only developed by banks, but also in collaboration with other actors or by third parties. Developments are market driven, and banks' customers expect to be

[1] In Norway, Finland, Sweden and Denmark there were not a single reported bank robbery during 2022 and 2023.

offered “state of the art” products and services, while also, rightfully, expecting high levels of consumer protection and security of transaction.

The requirements in PSD2 on strong customer authentication initially led to a decrease in card payments fraud. However, we now see a rapid and dramatic increase in social engineering fraud, where customers are tricked into authorising transactions by a fraudster. There are multiple methods for this, e.g., by telephone, e-mail, or text message, or even via home visits. The common denominator in the schemes is the attempt and desire to influence and persuade the bank customer to do something: click on a link, make a payment, or call a number. For example, a person might get an SMS telling them they have got a parking ticket that should be paid via an attached link.

In Sweden the number of “vishing scams”[2] reported to the police has increased by **555 per cent** since 2019. The median gain from vishing is much larger than that from card fraud. In Denmark the police report that fraud cases involving “smishing” has risen significantly, by approximately 130 per cent compared to 2022. The Danish police report an increase of IT-related financial crime since 2019 of 42 per cent in Denmark.

Combating fraud is a high priority for banks, who are devoting substantial resources towards protecting customers. We support the Commission’s initiatives that aim to facilitate information sharing, fraud monitoring and information campaigns, as a broad set of measures is needed to fight fraud in an increasingly complex landscape. This is a societal problem and all parties in the value chain (e.g., banks, payment initiators, social media platforms, internet and mobile providers, Big Techs, governments, and customers) need to acknowledge responsibility and to collaborate to make it as difficult for the criminals as possible.

Regulatory initiatives and preventive measures

1. *Payment service provider’s liability for impersonation fraud*
   We fear that the PSR proposal on payment service provider’s **liability for impersonation fraud[3],** when the fraudster for instance is pretending to be a bank employee, would support the criminal business model and could actually make the EU citizens more vulnerable to this type of fraud.

   A refund right for authorised transactions can make payment service users less concerned about security or lead to an increase in **"friendly fraud"** where the customer claims to be exposed to fraud, but in reality, is in collusion with the fraudster. This can in turn lead to an increased exploitation of young people and other vulnerable customers for the purpose of money laundering. Reduced attention to online risks could also spill over on all types of digital services and make payment service users more vulnerable to cyber risks.

   Incentives for other stakeholders (telecom and social media / online platforms) to collaborate with banks are eliminated when the full financial burden is carried by the banks. While banks invest heavily in fraud prevention, all parties in the fraud chain, including

[2] Most people have heard of phishing; vishing is a different attack that falls under the general phishing umbrella and shares the same goals. Vishers use fraudulent phone numbers, voice-altering software, text messages, and social engineering to trick users into divulging sensitive information. Vishing generally uses voice to trick users. (Smishing, yet another form of phishing that uses SMS text messages to trick users, is often used in tandem with voice calls depending on the attacker’s methods.)
[3] PSR article 59 with proposed amendments by the European Parliament

telecom companies and internet platforms, should be legally required to implement and collaborate on fraud prevention strategies and participate in the reimbursement of victims of these frauds.

2. *Telecommunication companies need to step up*
   Fraudsters are becoming increasingly good at mapping their intended victims in various target groups. The number of instances where our customers are defrauded by criminals exploiting weaknesses in the telecommunications networks is growing. Fraudsters conduct attacks such as **"spoofing"**[4] of telephone calls and text messages and send text messages with malicious content and text messages with the intend to phish the victim.

   These security weaknesses need to be addressed with increased regulation and oversight of the network security of telecommunications companies. Therefore, we advocate for stricter legislation that imposes greater responsibility on telecommunications companies to implement advanced security technologies and protocols. Telecom operators need to prevent that text messages or calls appear to come from a trusted party, while they in reality are sent by a fraudster. They also need to block text messages and spoofed numbers, to immediately block phone numbers used to commit fraud.

   Screening for bulk messages being sent including URLs is also needed. A European solution providing a register of aliases of SMS senders in order to avoid spoofing could be explored. We note several examples of national legislation, such as in Finland (where telecom companies report having prevented tens of millions of fraudulent calls), that are going in this direction, but we need to have it on a European level as well. A new requirement for telecom operators should be the introduction of an ad hoc protocol to allow them to verify the SMS sender.

3. *SoMe need to step up as well*
   Social media platforms have become fertile ground for financial crimes, facilitated by the prevalence of fake profiles and deceptive advertisements. In 2021, UK Finance carried out an analysis of nearly seven thousand authorised push payment scam cases. It showed that 70 per cent of scams originated on an online platform, highlighting the internet's significant role in enabling fraud. These fraudulent elements exploit the trust and engagement inherent in these networks, leading to scams and financial losses for unsuspecting users. To combat this growing threat, it is imperative that social media companies intensify their efforts in identifying and eliminating **fake accounts** and **misleading ads**. This could also include the implementation of more robust verification processes for profiles and more stringent review systems for advertisements.

   It is positive to see that the EU regulators have launched several investigations under the Digital Services Act to combat misleading advertisements, deepfakes and other deceptive information that is being maliciously spread online.

   We call for an obligation on internet platforms to control that the information provided is correct. They should also be obliged to verify the identity of their customers and assess their risk profile. Further measures that could be considered include the closure or

[4] 'Spoofing' is when fraudsters pretend to be someone or something else to win a person's trust. The motivation is usually to gain access to systems, steal data, steal money, or spread malware.

suspension of potentially fake / scam websites in a centralised manner, the revocation of the authentication web certificate of the website and stricter requirements during the verification process of hosting providers for opening a site.

4. *More information sharing is needed*
   One important tool in the fight against fraud is the **data sharing** between banks (and with other operators in society). Legislation that facilitates more data sharing between banks enables better risk assessments in both the preventive work and in the banks' transaction monitoring. The more information and data points the banks can share with each other, the greater the preventive effect. This approach involves exchanging critical data on fraudsters, incidents, and victims to identify and prevent fraudulent actions. We support the idea in the PSR regulation, but more is needed.

   We suggest setting up an EU wide data sharing network connecting all relevant EU and national financial and non-financial stakeholders. This EU network of networks should be used to share aggregated information comprehensively: statistical analysis of the most common types of fraud, new types of fraud, methods and techniques used by fraudsters and geographic area where the fraud took place. Real-time sharing of indicators of compromise (IoC) and indicators of fraud (IoF) and new manipulation techniques and other circumstances associated with fraudulent payments with the communities of stakeholders which can block fraud should also be shared in this network.

   First and foremost, the banks aim to share information about the so-called **mules**: name, personal identification number, address, phone number, and email, as well as details regarding the timing of account creation. This will facilitate tracking and halting fraudulent activities at an earlier stage.

   Additionally, the banks wish to share data about the incidents themselves, such as the date and amount of the fraudulently obtained funds, the used IP addresses, and device identifiers (Device ID), which could reveal if a fraudster operates across different banks. This information sharing will require security measures to ensure privacy and protect against data misuse.

5. *Information campaigns on EU level*
   The potency of proficient **social manipulation** should not be underestimated. The fraudsters are well versed in banks' products and technology, and in how payment clearing processes work.

   All parties in the payments value chain play a part in raising awareness of the potency of social manipulation. Methods change and develop as new countermeasures are being introduced. In several Nordic countries we are therefore undertaking large **information campaigns** to increase awareness, something that should be used in a wider scale on EU level.

   We see that our campaigns have positive effects, but awareness is not enough. In some Nordic countries, the pendulum is now swinging back, with societal calls for slowing down some of the clients' transactions, or at least for banks to provide for such options.

6. *EU's role in international judicial cooperation in combating large-scale fraud*
   Judicial cooperation within the EU, and above all between the EU and certain third countries, needs to be strengthened. A large portion of the organized fraud directed at EU bank customers are carried out by EU citizens located in third countries, which in many cases prevent intervention and an effective criminal investigation. It is not acceptable that fraudster networks can operate systematically from certain countries that do not cooperate with authorities in EU countries, exclusively targeting EU bank customers. Given that it can be difficult for many EU countries to establish bilateral judicial cooperation with these third countries, the EU needs to facilitate such cooperation at a central level. The EU should exert pressure on third countries that systematically harbour "EU fraudsters". Increased activity by Eurojust could play an important role in this.

7. *Definition of authorisation in PSR*
   The current policy discussion around the definition of **authorisation** – and especially the amendment proposed by the European Parliament – would create legal uncertainty and fragmentation in EU payments regulation, undermining the well-established civil liability framework between payment service providers and payment service users. We therefore fully support the concerns raised by the European Banking Federation (EBF) in the **attached position paper**. Introducing a subjective element for authorisation would enable payment service users' claim for a refund in any transaction, undermining the need for risk assessment and control. Subjective elements should be avoided at all costs to prevent legal uncertainty entering the payment ecosystem.

Continued dialogue
Against this background, The Nordic banking associations would like to underline the need to strike the right **balance** between, on the one hand, immediate availability to payment and transaction services, and, on the other hand, the protecting of the safety of the customer.

We hope that our experience as frontrunner digitalised economies will serve as an example of the need to safeguard this balance.

The Nordic Banking associations stand ready continue the **dialogue** on these matters and convey our experiences, as well as counteractions. We are convinced that these crimes are best fought with awareness and the right legal framework, especially with a close cooperation between the regulators, the law enforcement authorities, and the industry.

Kind regards

Ulrik Nødgaard
Finance Denmark

Arno Ahosniemi
Finance Finland

Kari Olrud Moen
Finance Norway

Hans Lindberg
Swedish Bankers' Association