Improved payment security implies innovation in authentication

SMS authentication codes should disappear but multi-factor authentication needs acceleration

Lars Jacobs MSc
is a manager at KPMG.
jacobs.lars@kpmg.nl

Kristel van Pinxten MSc
is a consultant at KPMG.
vanpinxten.kristel@kpmg.nl

Innovation in the online payment sector should go hand in hand with innovation in authentication. There is a battle against cyber payment fraud, which requires improvement in authentication methods used. With regulation like the second Payment Service Directive, regulatory requirements have been introduced, which set minimal security requirements. Multi-factor authentication and the dynamic linking of authentication codes are actions that should be looked into. At the same time, the customer journey should be optimized without losing sight of security concerns. How can cyber security of payment systems be ensured by using the right multi-factor authentication methods? This article contains advice from professionals regarding the protection of online payment systems.

INTRODUCTION

Multiple innovative online payment services and business models have emerged, encouraged by new regulation, such as the second Payments Service Directive (PSD2) in Europe. Additionally, there has been a significant increase in cyber fraud in the banking and payments sector. According to research from Betaalvereniging Nederland, the damage of cyber fraud in internet banking more than doubled from €3.81 million in 2018 to €7.94 million in damages in 2019 in the Netherlands alone ([Beta20]).

This has been accompanied by a spike in e-commerce and the rise of mobile-first, resulting in a gradual transition in the way consumers use online services. Customer centricity drives this. But at the same time, it raises concerns about security and the way consumers authenticate themselves online for these new innovative services.

Cyber criminals are professionalizing in the payment domain. The European Payments Council stated this in its recent report, highlighting the current threats and fraud trends ([EPC19]). Among the trends noted, authentication and activation are common themes. It is very important to stay ahead of the way financial institutions regulate their authentication to ensure security. This is because the right authentication method can add an additional layer to the protection of sensitive data. In 2018, PSD2 was introduced, which set requirements for authentication and created new innovative possibilities in the payment sector. However, cyber criminals have also become more inventive in finding accessible ways of bypassing authentication methods, especially when using SMS-based authentication. Hackers trick phone companies into swapping a phone number to a new device, so-called SIM swapping. In this way, hackers do not need the actual device to receive the two-factor authentication codes for both financial and other services that the consumer uses. Without the right authentication methods, data breaches can occur easily and lots of money and sensitive information can be lost. Therefore, payment security goes hand-in-hand with innovation in authentication for all online services.

While companies in the financial sector are under pressure to ensure the safety of the sector and their consumers, this article takes a broader perspective. When protecting the payment and banking industry and ensuring secure online authentication, we need to look beyond this industry. This is because safe online authentication is relevant to all online services to protect the (personal) information in these services. This article starts with exploring the opportunities for innovation in payments, followed by security-centric journey optimization, cyber fraud and the right direction of authentication. In this article, questions concerning security will be discussed, such as: "How do we balance the opportunities for enhanced customer experience with the security concerns of cyber fraud?", "Why is the online two-factor authentication using SMS, both within and out of the banking sector, a key concern?" and "Why does the SMS-based two-factor online authentication remain common practice in the industry for online authentication, while it brings a lot of security risks?"

PSD2 OFFERS OPPORTUNITIES AND SECURITY

In 2018, PSD2 was introduced and gave options to use new online payment system services. The introduction of PSD2 in 2018 increased the opportunities for innovation in the online payments space even further than was already the case ([EPoC15]). PSD2 made it possible to give access to payment accounts to third parties, with the consumer's explicit consent, resulting in access to payment accounts anywhere and anytime.

New business models are, therefore, emerging, resulting in new companies, while other existing companies are developing in-house payment capabilities so that elements of their payment value chain can be integrated into their business. A plethora of FinTechs have emerged, acting at the intersection of consumers, retailers and banks, offering third-party payment services (e.g. initiation of payments on behalf of customers). For example, payment service providers (PSPs) or banks such as Adyen are active in the market between consumers and retailers, offering a variety of services to facilitate online payments. In parallel, large technology companies (BigTech), such as Google, Apple and WeChat are also entering the world of payments. This results in innovation opportunities and optimization of services.

As well as enabling innovation, PSD2 aims to tackle fraud in online payments ([EC19]). The regulation strengthens the security requirements for electronic payments. "Strong customer authentication", as well as the subsequent dynamic linking of authentication codes to payment transaction details, are key elements of PSD2 security requirements. PSD2 mandates that strong customer authentication is used. This is defined by the European Parliament and European Council as "*an authentication based on the use of two or more elements categorised as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is) that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data*"([EPoC15]). In this way, PSD2 regulation ensures that companies offering payment solutions must ensure at

least two-factor authentication of their customers. The dynamic linking requires that an authentication code for each transaction needs to be unique, as it can only be used once. It will be specific to the transaction amount and recipient, and both are clear to the payer during authentication ([Saee18]). These elements aim to reduce the risks of cybercrime-based fraud.

PSD2, in this way, presents opportunities for innovation, optimization of customer experience and security improvements. However, the optimization of customer experience and the security of online payments ecosystem as a whole will be a challenging line to walk.

The importance of authentication to cyber payments fraud

Case study example illustrating the risks of SMS-based two-factor authentication

A cyber criminal calls the phone company in your name and acts as if you are moving to a new phone that requires a smaller SIM-card, or so the cyber criminal says. The helpdesk asks for a few personal details: name, date of birth, address. The cyber criminal makes sure to update "your" address while on the phone and in no time the cyber criminal has received "your" new SIM-card. Only they are not you, they are committing fraud...

How did this cyber criminal know the victim's name, date of birth and address? Or their mobile provider? Cyber criminals use social engineering techniques to receive as much information on the person as possible. This cyber criminal could easily find the victim's name and date of birth on social media. Having attained access to a set of email addresses and passwords hacked last year, the victim's home address was also easily found within a forgotten email inbox, along with a vast number of other items, including their mobile service provider and even a copy of their passport. Now able to access someone else's One-Time Passwords (OTPs) and Mobile Transaction Authorization Number (MTAN) sent through an SMS, via this new SIM-card, this cyber criminal was ready to execute fraud and interfere in the payment transactions of the victim. The data breach that occurs from such SIM-based attacks may result in the loss of a large amount of money or sensitive personal data.

This case study example highlights this growing trend and the dangers of SMS-based two-factor authentication. Whereas in the past this type of SIM-swap fraud was used to call premium numbers, today the risks are greatly increased as companies use codes via SMS to implement two-factor authentication. This type of fraud has cost British banks around £91 million (€108.2 million) over the last 5 years ([Wrig19]).

The safety and effectiveness of two-factor authentication is therefore highly dependent on the authentication solution deployed across use cases, i.e. not just in the banking and payments sector but also to other online services in which consumer data is stored.

Not all two-factor authentication is equal in their security. The use of SMS-based authentication, although notably the most commonly used type online, should be phased out. A weak link like SMS-based authentication can lead to a snowball effect on individual and company cyber security.

Optimizing security and the customer experience: a fine line

There is an ever-increasing demand from general consumers for an excellent customer experience ([Wich19]). As companies try to improve all aspects of their customers' experience and journey, it is increasingly important to seamlessly integrate actions that are not central to the product/service experience. As such, the seamless integration of payment transactions within a purchase or service is becoming the norm. An example of this is an electronic "wallet" and loyalty services offered in tandem. Uber, who recently received an electronic money license from DNB, is a prime example of the value chain integration ([FD19]). In the Uber Cash payments experience no user action is required to pay for the service at the point of use. This can also be enabled by the Uber Cash wallet, which is an option alongside the seamless credit card option. The payment becomes invisible – this fundamental shift in the perception of transactions requires a shift in the approach to security.

Not all customers are aware of the importance of the steps they need to take to ensure security. Often, customers are not aware of the high possibility of a data breach, when not using the correct cyber security measures. Every extra step in a customer's journey, including the payment and associated cyber security steps, can create an opportunity for the customer to stop their purchase and leave the online retailer website – a missed sales conversion. The benefits of decreased cyber fraud risk are hardly visible to the consumer. This is a fine line that established banks, new players as well as e-retailers and the rest of the online ecosystem are walking today – secure strong customer authentication is an absolute must, but how can this fit seamlessly in the customer's experience? Multi-factor authentication should be seen not as about adding steps

but as about adding the right steps. As an example, when using multi-factor authentication, such as face recognition, this adds a step that is more secure than an SMS code, but that does not necessary feel like additional steps from the consumer perspective.

Strangely enough, online authentication methods have changed little when compared to the rate of digital, technical and payment-related innovation over the last few years. Most people are still accustomed to logging in using a username and a password. However, according to research from Duo, due to a combination of an increase in (media) awareness and the introduction of regulation such as PSD2, two-factor authentication is increasingly used by consumers online. The most common form is a combination of a "knowledge" element (login details, i.e. something only you know) and a "possession" element (a code via SMS, i.e. something only you have) ([Duo19]). The "inherence" category, for example the use of biometric data such as a fingerprint, is beginning to become the standard, especially where mobile devices provide this functionality.

The continued implementation of SMS-based authentication for two-factor authentication in the online context is a prime example of a well-intentioned attempt to find the balance between facilitating a streamlined consumer journey and enhancing security. When consumers are already on their mobile phone or have it with them all the time, it seems easy to also receive an authentication code via their phone and SMS. However, as the emerging (cyber) threats highlight, including those in the aforementioned case study, SMS-based two-factor authentication does not imply guaranteed cyber security. These cyber threats are explained in more detail in the next section.

CYBER FRAUD AND THE PAYMENTS ECOSYSTEM

Phishing, social engineering and Advanced Persistent Threats (APTs – a long term form of cyber fraud that uses multiple combined techniques) are a handful of possible cyber threats in the payment ecosystem. When it comes to SEPA transactions, the primary cause of fraud losses remains the use of impersonation and deception scams and attacks to compromise data, according to the European Payments Council. Increasingly, cyber criminals are targeting mobile devices along with IoT devices. Attacks can include, for example, Banking Trojans, a form of malware targeted at the victim's online and/or mobile banking activities. Transactions can be tampered with or user authentication credentials could be stolen. Additionally, phishing for activation codes for mobile payment and authentication apps will likely increase over the coming period, using techniques such as social engineering.

Card payments are influenced by a trend towards more technically sophisticated fraud techniques such as APTs, characterized by their long-term, persistent and often long-undetected nature. At the same time, it is noticeable that cyber criminals are also increasingly employing simpler fraud types such as reporting a card lost or stolen to gain access. This is sometimes combined with social engineering, which is on the rise along with phishing attacks. The case study earlier shows an example of a combined approach, with SMS-based authentication as the central weak link.

Within businesses, these attacks often come in combination with malware. Research of Internet Crime Complaint Center (IC3) reported that Business Email Compromise(BEC)/Email Account Compromise (EAC) – a scam targeting businesses or individuals compromising email accounts through social engineering or computer intrusion techniques to conduct unauthorized transfer of funds – cost American businesses adjusted losses of over $1.7 billion (€1.56 billion) in 2019 ([IC319]).

The European Payments Council also highlights that social engineering attacks and phishing are also trending to include not only consumers, retailers and small-medium sized enterprises, but also employees, financial institutions and payment infrastructures. This leads to an increase in authorized push payments fraud in which the payment is authorized by the victim.

This context highlights the fact that cyber fraud in payments is influenced across an ecosystem of online services within the payment and banking industry and that this type of authentication has a significant impact on the security measures.

Who is prepared and who is responsible?

On an optimistic note, larger banks seem to be better prepared. When it comes to cyber fraud and the deployment of multi-factor authentication, the process of phasing out SMS-based authentication has been initiated by multiple larger consumer banks, such as ING. Biometric options for multi-factor authentications, such as touch ID or face recognition, have also been introduced within mobile banking apps. This is a good example of banks taking advantage of innovations in mobile phones and security, introducing an inherent element (something you are) to their multi-factor authentication options. However, small banks, such as private banking and savings banks, are traditionally lagging behind in these developments and many still use SMS-based authentication. This, in combination with their customers generally being limited in their awareness of cyber risks, leaves smaller banks more vulnerable to the cyber risks arising from phishing attacks and social engineering.

The case study example includes the phishing of customers to gain access to their mailbox that is configured without two-factor authentication. Even if the mailbox had been secured with SMS-based two-factor authentication, acquisition of the SIM-card as per the case study could also have ensured access to the victim's mailbox too. Sensitive documents often reside in personal mailboxes. These types of documents are often used by organizations to verify the identity of a caller, such as copying passports or bank account statements. The bypassing of verification controls resulting from too much focus on customer friendliness enables "attackers" to request duo SIM-cards that are then sent to an alternative postal address. With the additional SIM-card, the attacker can start the request of SMS-based authentication and/or password resets in order to gain access to payment and online banking portals. From the control and process perspective of the mobile service provider this is all legitimate, as the verification of personal sensitive information was successful. This demonstrates that while some financial institutions are prepared, others outside this sector have a role to play in security.

Currently, banks are mostly seen as the responsible organizations for cyber fraud. This is a result of the position of banks as the keepers of the consumers' money. The current payment space, however, is inherently an ecosystem by nature. Not only banks, but also e-retailers, email service providers, mobile service providers and so forth are active in this cross-sector ecosystem of security. The responsibility of the choice of authentication technique should be shared across all of them.

OUR EXPERIENCE ON SOLVING CYBER INCIDENTS IN THIS CONTEXT

The result of the fraud in payment systems often results in loss of large amounts of money and sensitive data. There is a need to understand how to deal with emerging technologies embedded in business processes and customer journeys. This turns cyber security challenges into real business enablers. Having a multidisciplinary cyber response team can assist in preparing and adequately dealing with cyber security risks when these materialize. In KPMG's experience, forensic and cyber experts combined have capabilities that can be deployed in tandem as a response to cyber threats. Dealing with a cyber security breach is often a deep technical topic that involves technical specialists and technical jargon. A functional approach is to bring it back down to essential management questions, to be able to adequately respond to a cyber security breach and provide the insights that matter.

Sensitive documents often reside in personal mailboxes

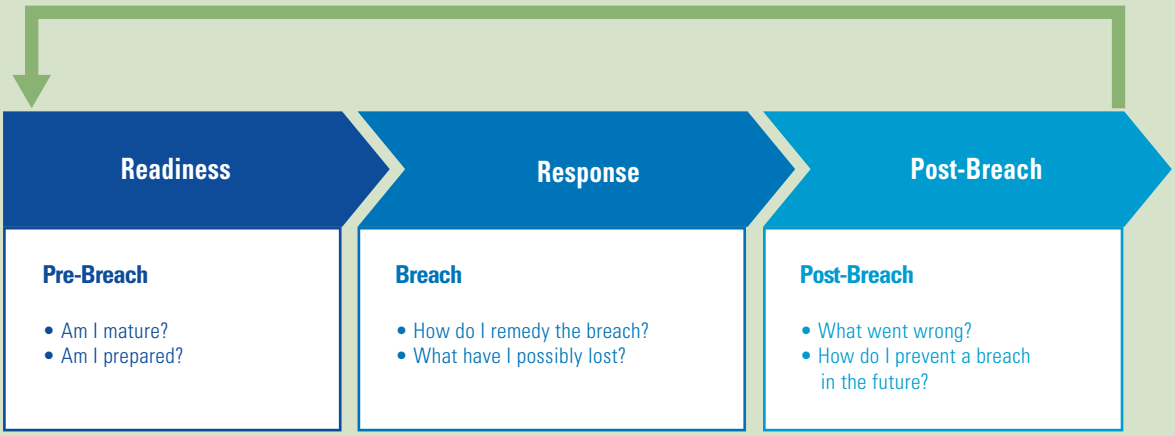

Figure 1. Three phases identified to adequately deal with a cyber security breach.

The first phase, readiness, is to focus on adequate design, implementation and limit the damage of breaches by effectively planning for possible cyber security incidents. One of the main aspects is to assess the current state of an incident response. This helps address the gaps so that processes can be improved, tools can be implemented, strategic partners can be selected and staff can be trained.

The second phase, response, is where the cyber response team comes into action. It is all about mitigating the impact of a cyber incident. Activities such as forensic data acquisition, system and log file analysis and incident management are to be executed in this phase.

In the third phase, post-breach, the root causes need to be identified and mitigations must be successfully applied. In regulated industries or if breach concerns personal data, the GDPR regulation imposes legal obligations to report the cyber incident to the regulator. Strengthening an organization's detection and response capability are important aspects to consider in this regard. These could be temporarily strengthened as cyber criminals may still have presence in the organization's network.

AN OUTLOOK TO THE FUTURE OF AUTHENTICATION MECHANISMS

Due to the methods used by cyber criminals, not using multi-factor authentication is like closing the door of your home but not locking it. Crimes such as business email compromise, data theft and phishing can be prevented when changing to multi-factor authentication. Multi-factor authentication requires dynamic linking of two pieces of unique personal data that ensures someone's identify. This is more detailed than the SMS two-factor authentication, as discussed in this article.

A move towards multi-mode biometrics is expected in the future. This combines identifiers, such as fingerprints and gait analysis (behavior) to produce high-reliability biometrics matching. Eventually, silent authenticators will be incorporated and one will not have to actively present oneself, but will be automatically recognized based on machine learning algorithms which will combine multiple biometric factors and gait analysis. Such behavioral biometrics can help prevent identity theft, protecting the property of individuals. The combination of something only one person can "know", and typical behavior, can help exclude criminals from the lives of people.

The awareness of having innovative authentication methods across industries is crucial for cyber security.

CONCLUSION: INNOVATION EVERYWHERE

Cyber criminals are innovating. The online payment sector is innovating. There should be a wider movement to innovate online authentication methods. It is advised to integrate new technologies in the cyber security sector into the complete journey of the consumer. Besides innovation in the services offered online, this also means innovation in the security that comes with these new services.

The embedding of multi-factor authentication and the dynamic linking of authentication codes to the payment transaction details in PSD2 legislation, is promising. It provides the backbone for this next phase of authentication and the battle against cyber fraud in payments. Authentication presents itself as a bottleneck issue in this process, especially when society moves further and further into a fully digital life.

Innovation in payments must therefore go hand in hand with innovation in authentication. Implementing the core principles of multi-factor authentication must be placed in context of the entire customer journey: how does security impact the consumer (online) and how safe is the authentication choice that has been made in this context? To protect the payments industry, protection of consumers across platforms is needed, both within and outside the banking and payments industry. The first step is through the elimination of SMS-based authentication and the true implementation of multi-factor authentication, including the combinations of factors that are less vulnerable to fraud.

References

[Beta20] Betaalvereniging Nederland (2020, April 16). Veel meer phishing en bankpasfraude in 2019. Retrieved from: https://www.betaalvereniging.nl/actueel/nieuws/phishing-bankpasfraude-2019

[Duo19] Duo Labs (2019). *State of the Auth.* Retrieved from: https://duo.com/assets/ebooks/state-of-the-auth-2019.pdf

[EC19] European Commission (2019, September 13). Frequently Asked Questions: Making electronic payments and online banking safer and easier for consumers, Retrieved from: https://ec.europa.eu/commission/presscorner/detail/en/QANDA_19_5555

[EPC19] European Payments Council (2019). *2019 Payment Threats and Fraud Trends Report.* Retrieved from: https://www.europeanpaymentscouncil.eu/sites/default/files/kb/file/2019-12/EPC302-19%20v1.0%202019%20Payments%20Threats%20and%20Fraud%20Trends%20Report.pdf

[EPoC15] European Parliament and of the Council (2015). Directive (EU) 2015/2366. *Official Journal of the European Union.* Retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L2366&from=EN

[FD19] FD (2019). Uber krijgt vergunning DNB voor uitvoeren elektronische betalingen. Retrieved from: https://fd.nl/ondernemen/1296128/uber-krijgt-vergunning-dnb-voor-uitvoeren-elektronische-betalingen

[IC319] Internet Crime Complain Center (2019). *Internet Crime Report.* Federal Bureau of Investigation. Retrieved from: https://pdf.ic3.gov/2019_IC3Report.pdf

[Saee18] Saeed, N. (2018, December 19). Understanding Dynamic Linking in PSD2. Twilio Blog. Retrieved from: https://www.twilio.com/blog/dynamic-linking-psd2

[Wich19] Wichers Hoeth, N. (2019). *A digital walk to remember.* KPMG. Retrieved from: https://assets.kpmg/content/dam/kpmg/nl/pdf/2019/advisory/a-digital-walk-to-remember-2019.pdf

[Wrig19] Wright, M. & Horton, H. (2019, November 30). Bank Customers Lose £9.1 Million In Five Years To 'Sim Swap' Scams. *The Telegraph.* Retrieved from: https://www.telegraph.co.uk/news/2019/11/30/bank-customers-lose-91-million-five-years-sim-swap-scams/

About the authors

Lars Jacobs MSc is a manager within KPMG's Forensic Technology team in the Netherlands. He has a background in digital forensics, network architecture and IT-audit. Lars helps his clients to gain insights into the facts and reconstruct the events of a cyber security incident. This will enable them to take the right actions.

Kristel van Pinxten MSc is a consultant within KPMG's Forensic Technology team in the Netherlands. She finished her master's degree at the Erasmus University Rotterdam. Her thesis covered the profiling of employees to prevent possible non-compliant behavior with cyber security rules. Additionally, she worked within a sub-division of the Royal Netherlands Navy as the person responsible for information management.