FINDINGS OF RESEARCH CARRIED OUT BY FINEXTRA IN ASSOCIATION WITH MITEK

JUNE 2018

MEETING EU REGULATORY REQUIREMENTS IN A POST DATA BREACH ERA

Mitek | Finextra

CONTENTS

01 INTRODUCTION

2017 played host to a catalogue of data breaches, and some of the most shocking examples were those that were an updated account of previously reported breaches. This has done nothing to augment already dwindling trust in financial services. In the wake of the second Payment Services Directive (PSD2), the General Data Protection Regulation (GDPR) updates and Anti-Money Laundering (AML) updates with their regulatory requirements for stronger verification and more rigorous data protection, have current verification methods passed their expiry date?

The plethora of digital account services available now has given rise to more opportunities for cyber criminals to breach customer account data- this can then be sold on the dark web and used for fraud and money laundering. At the same time the rise of cryptocurrencies has enabled such nefarious activities by providing anonymity. What is the way forward for digital payment and service providers to know exactly who their customers are as they come under increased regulatory scrutiny?

Traditional verification checks such as knowledge-based authentication (KBA) are losing credibility as so much customer information is now stored online and can be pieced together by fraudsters. What new methods can these outdated ones be replaced with, and how best can financial institutions tackle the growing problem of increasingly sophisticated and large-scale attacks? As payment services companies large and small try to come to grips with knowing their customer to satisfy upcoming regulation, they need to make sure they don't alienate the customer while creating a compliant onboarding process. On top of that challenge, they also need to be sure that they can achieve compliance at a reasonable cost with a good user experience.

This white paper, produced by Finextra in association with Mitek, explores these issues and highlights some of the emerging methods financial institutions can deploy to meet compliance obligations while onboarding their customers in a secure, and, most importantly, user friendly manner.

Enhanced European regulation requiring stronger due diligence

Increased incidences of data breaches and money laundering have led to a further recalibration of European anti-money laundering regulation.

Key Highlights of the Fourth European Anti-Money Laundering Directive (AMLD)

Replacing the EU Third Anti-Money Laundering Directive, this fourth iteration, enacted on 25 June 2015 and implemented 26 June 2017, features the following highlights:

- Emphasis on ultimate beneficial ownership and enhanced customer due diligence (CDD)
- Expanded definition of a politically exposed person (PEP)
- Cash payment threshold lowered to €10,000
- Expanded to included entire gambling sector beyond just casinos
- Enhanced risk-based approach, requiring evidence-based measures

Ever-more detailed requirements in relation to customer identification and verification are asked of financial services providers and electronic money products and cash payments over the value of 10,000 are subject to enhanced scrutiny. The need for accurate and up-to-date information on the beneficial owner is a key factor in tracing criminals who might otherwise hide their identity behind a corporate structure, says the regulation. Increased due diligence is therefore required, and traditional methods of identity verification are no longer secure enough. With reference to ultimate beneficial ownership and politically exposed persons, in short, FS and payments firms need to have a robust, holistic and auditable view of their customer in order to understand their liability over customer funds and the entire history thereof

In terms of identity verification measures, Know Your Customer (KYC) and Customer Due Diligence (CDD) methods need to be tightened to prevent the exploitation of the financial system for money laundering and terrorism financing purposes. CDD pertains to identification and verification of a customer from documents, data or information obtained from a reliable and independent source.

Enhanced Due Diligence (EDD) techniques such as electronic signatures and facial recognition are being brought into the onboarding process in order to satisfy AMLD4.

The second Payments Services Directive (PSD2) has mandated FS firms to implement SCA (Strong Customer Authentication), involving a multifactor system of customer identification to enhance KYC.

02

DATA BREACHES DRIVING MORE DETAILED REGULATION FOR ENHANCED IDENTITY VERIFICATION

In the last few years, the number of high-profile security breaches has ramped up considerably. However, this past year took the era of data breaches to a new height. Global corporations such as Uber, Yahoo, data bureaux such as Equifax and major corporations such as Deloitte all came under fire for large-scale breaches that have severely knocked consumer trust and brought once-secure identity verification methods under the spotlight.

Uber

In November 2017 Uber announced that information from 57 million customer accounts had been compromised as well as that of 600,000 drivers. The company said it had taken immediate steps to identify the individuals and obtain assurances that the downloaded data had been destroyed and that the company had also strengthened its cloud-based storage accounts. Details such as names, email addresses and phone numbers were included in the breached data, as well as driver licence numbers. Uber reportedly paid $100,000 to the hackers to delete the data and keep quiet about the breach.

Equifax

In early September 2017, Equifax's US parent company announced it had fallen prey to a criminal cyberattack in which 143 million user accounts (of which 15.2 million were UK records), dating between 2011 and 2016, were attacked. In addition, it said credit card numbers for about 209,000 US consumers and dispute documents with personal identifying information for approximately 182,000 US consumers were also breached.

Four risk groups were determined around the different types of information accessed: email, membership details, such as username, password, secret questions and answers and partial credit card details; drivers' licence and phone number.

Yahoo

In October 2017 it emerged that a Yahoo hacking attack dating back to 2013 had affected "all of its three billion user accounts", three times the number it had previously announced. The revelation came to light when the company was taken over by Verizon. It stated that the stolen information "may have included names, email addresses, telephone numbers, dates of birth, hashed passwords (using MD5) and, in some cases, encrypted or unencrypted security questions and answers but did not include passwords in clear text, payment card data, or bank account information. Payment card data and bank account information are not stored in the system the company believes was affected."

Deloitte

Deloitte was hit by a data breach at the latter end of 2017, revealing that an attacker compromised account credentials and gained access to a single Deloitte cloud-based email platform. The company said this system was distinct and separate from other Deloitte platforms, including those that host client data, collaborative work among Deloitte professionals, engagement systems and other non-cloud based email systems. It said, "the attacker was specifically focused on obtaining active credentials".

Deloitte was in the process of rolling out multi-factor authentication; and has since completed this. While the breach affected "very few clients", the high profile of its global consulting operation intensified the growing concern regarding the threat of cyber-attacks over the course of 2017.

This succession of increasingly alarming data breaches is indicative of a rapidly changing environment, in which old measures such as KBA (Knowledge Based Authentication) are becoming less effective. Data acquired from large-scale breaches are made available on the dark web and sold for criminal activity. The kinds of data breached and sold are those used for traditional KBA- answers to security questions such as mother's maiden name, family pets, favourite colour, etc. As a result, stronger and more personal KYC techniques must be employed. Further to this of course is a sophisticated, user-centric paradigm, driven by major online brands, not bound by the same rules as financial providers but setting the benchmark for frictionless customer experience.

03

KNOWLEDGE-BASED AUTHENTICATION (KBA) WEAKENED AS A RESULT OF LARGE-SCALE DATA BREACHES

Historically an indispensable tool in a layered identity verification process, KBA -has become increasingly weak. KBA confirms someone's identity through a series of questions. The answers must be compared with the data held, from a reliable source. On its own, this is weak, and has become even weaker, due to the various methods through which this kind of information can be sourced online by fraudsters.

Answers to questions such as mother's maiden name or family history may be obtained from scouring online genealogy sites such as ancestry.com. Equally, personal history information can be obtained from school reunion sites. "Even answers to questions like who your favourite teacher was can be gleaned from polls classmates have participated in; polls you didn't even answer," says Doug Franklin, research technologist at IBM Security X-Force.

"Do we need to mention the treasure trove of information the likes of Facebook and LinkedIn afford the persistent hacker? And the numbers of organisations that have such KBA information about their users stored over the years," continues Franklin. It is after all only recently that the notion of the right to forget has come into play.

The growth of digital banking has yielded many benefits and many challenges. On the darker side of the digital transformation, digital services have facilitated the growth of ever-more sophisticated money laundering schemes. Digital banking enables anonymity and the myriad new payment instruments has created new opportunities for fraudsters also, not to mention the nefarious portals cryptocurrencies lend themselves to. Data breaches have become in large part the first step in a fraud cycle. Large stolen data sets are sold online enabling more insidious instances of fraud and money laundering.

04

COMPLIANCE AS AN OPPORTUNITY FOR COST-SAVING, DIGITAL TRANSFORMATION AND CUSTOMER SATISFACTION

Quite apart from the ethical standpoint of keeping customer accounts safe, the sheer costs involved when not abiding by the rules are prohibitive at best, fatal at worst. In early 2018, US Bancorp was ordered to pay the eye-watering penalty of $613m on behalf of its subsidiary US Bank for inadequate AML checks. The organisation was deemed to have "wilfully" violated the Bank Secrecy Act in failing to report suspicious activity as per protocol.

In a Gartner report, objectives are set out as to the new paradigms of AML processes, including stringent KYC checks, methodical reporting for large currency transactions, as well as verifying individuals or businesses involved in transactions and transaction monitoring.

To implement a thorough AML process is no easy feat, but it satisfies three fundamental issues for PSPs: compliance, fine avoidance and preservation of reputation and customer trust. Additionally, as individuals responsible for compliance within companies can now also be held personally responsible and receive fine and/or jail time, being on the right side of the regulation is now very important.

PSPs and financial providers need to tackle this perfect storm for several reasons over and above protecting their livelihood and reputation- to assuage growing customer concern, reduce risk and therefore cost, and retain a loyal and happy customer base founded on trust and transparency.
While GDPR and PSD2 provide a large stick which spurs compliance, the regulations also offer a carrot for those PSPs and FI's who drive towards more investment in digital and compliance.

A recent Finextra survey found that 86% of bank respondents said their banks have a "strategic objective to leverage PSD2 as an opportunity to innovate, differentiate and create new products and services" (with 58% strongly agreeing).

Further to this, 68% of respondents agree or strongly agree that their ability to invest in PSD2 has enabled them to speed up their digital transformation programme.

The maximum fine that can be imposed as a result of breaching GDPR is €20m, or 4% of the company's annual turnover, whichever is the greater. If an individual's privacy rights are infringed, in terms of consent of data processing and lawfulness regarding the use of a subject's data, this can incur the top fine. And there is industry-wide recognition that regulators will look to make an example of businesses which fail to comply.

There is a lower tier fine, which is up to €10m, or 2% of annual global turnover, whichever is higher. Data security breaches, or infringements of an organisation's obligations would incur the lower tier fine.

Another benefit of the early-bird-gets-the-worm approach to adapting to the newest regulations, and a large part of GDPR enforcement, is to what extent the organisation can prove intent to comply. If this is clear, it can go a long way in terms of reducing punitive measures.

Tightened regulation now means that penalties can be brought against financial institutions and individuals therein for violations of Suspicious Activity Reporting (SAR) rules. This makes it even more crucial for PSPs and financial providers to know their customer from the outset and not have to consider such consequences.

In January 2018, The European Parliament and Council agreed a set of rules to make users on cryptocurrency exchange platforms identifiable instead of anonymous, as was previously the case. The decision came in the wake of terrorist attacks, which EU officials said were facilitated by the anonymity afforded by cryptocurrency, and the Panama and Paradise Papers leaks. The rules also limit the use of prepaid cards and increases transparency around transactional information when there is legitimate interest to access the data.

The action will likely trigger individual companies to implement stronger verification methods above and beyond compliance, as awareness is increased, and action is required to reinforce customer trust.

05

STRONG CUSTOMER IDENTITY VERIFICATION- WHAT CAN BE DONE

One of the most impactful PSD2 mandates is around strong customer authentication, and two-factor authentication will now be required for all electronic payments, with exceptions to accommodate 'frictionless flow'. Two-factor authentication is based on two or more elements of Knowledge, Possession and Inherence. More casually, these three categories can be described as something a customer knows (password), something a customer has, for example an ID document, and something a customer is (a biometric feature, such as facial features). Under the EBA guidelines, the requirement to perform SCA applies to internet payments, building a need for digital identity verification for both account opening and regulated transactions.

As more and deeper checks are required, and the audience for them expands, PSPs and financial institutions are left to their own means to navigate the increased verification costs and customer experience demands, while maintaining top line growth.

"We have to balance regulations and market forces: data breaches or payment industry opportunity and customers. The cost of regulatory checks will increase dramatically, particularly for payment providers or FIs that rely on insufficient processes or manual intervention. Digital identity verification as an opportunity to achieve compliance, deliver a good customer experience less expensively growing revenue thank," Mitek's Hendrikse pointed out.

What's required is digital multi-factor verification. - One secure way to identity your customer is ID document verification paired with biometric facial comparison. This is done by asking the customer to take a photo of an identity document and a selfie. This allows financial institutions to know that the person on the other end of the digital device is presenting an authentic government issued ID document to identify themselves. The selfie is then used to verify that and the very person presenting the ID is actually the person presenting the ID document. I f invested in and well executed, the result is a frictionless user experience, far preferable than KBA for verify the identity of a customer to achieve compliance with regulations.

06
CONCLUSION

While adhering to increasingly stringent customer identification measures will prove to be an ongoing challenge for payment service providers in the wake of PSD2 and GDPR, it is simply the natural evolution of the industry and should be seen as an opportunity for PSPs to get a grip on the identity verification strategy, in turn strengthening their customer base in the increasingly important digital channel.

The fear is that increased identity verification processes will result in customer attrition, and while there is plenty of research and evidence to support this fear, it is not the case that there is nothing to be done to offset it. Customer education is key, and payment industry stakeholders should collaborate with each other more on best practice, and the technical standards and regulatory powers-that-be can and likely will do more to clarify implementation of new processes as the new era of PSD2 and GDPR unfolds.

Knowing your customer is more than ever about knowing not only that the identity document the person presents is indeed authentic, but also that the person presenting it is the person it identifies. Tougher AML requirements brought in by the EU means the cost of KYC for banks has increased significantly.

“The message to all financial institutions is clear: The cost of KYC checks is much too high, placing too much reliance on inefficient and error-prone manual processes,” said Steve Pannifer, COO, Consult Hyperion. Strong, seamless, multi-factor identity verification is crucial as part of a more comprehensive KYC strategy to protect both customer and business against money laundering while satisfying the regulators. If payments firms can harness technology to implement the right methods to satisfy AML and PSD2 regulations as well as the continual customer demand for a smooth and secure experience, they stand to reap all the rewards the open banking arena was designed to generate and avoid the triple threat of customer attrition, punitive fines and brand reputation.

07 ABOUT

Finextra

This report is published by Finextra Research.

Finextra Research is the world's leading specialist financial technology (fintech) news and information source. Finextra offers over 100,000 fintech news, features and TV content items to visitors to www.finextra.com.

Founded in 1999, Finextra Research covers all aspects of financial technology innovation and operation involving banks, institutions and vendor organisations within the wholesale and retail banking, payments and cards sectors worldwide.

Finextra's unique global community consists of over 30,000 fintech professionals working inside banks and financial institutions, specialist fintech application and service providers, consulting organisations and mainstream technology providers. The Finextra community actively participate in posting their opinions and comments on the evolution of fintech. In addition, they contribute information and data to Finextra surveys and reports.

For more information:

Visit www.finextra.com, follow @finextra, contact contact@finextra.com or call +44 (0)20 3100 3670

ABOUT

Mitek

Mitek a global leader in digital identity verification solutions built on the latest advancements in AI and machine learning. Mitek's identity verification solutions allow an enterprise to verify a user's identity during a digital transaction. This enables financial institutions, payments companies and other businesses operating in highly regulated markets to mitigate financial risk and meet regulatory requirements while increasing revenue from digital channels. Mitek also reduces the friction in the users' experience with advanced data prefill and automation of the onboarding processes. Mitek's innovative solutions are embedded into the apps of more than 6,100 organizations and used by more than 80 million consumers.

For more information, visit www.miteksystems.com or www.miteksystems.co.uk.

Finextra Research Ltd
1 Gresham Street
London
EC2V 7BX
United Kingdom

Telephone
+44 (0)20 3100 3670

Email
contact@finextra.com

Web
www.finextra.com