THE PAYPERS

Web Fraud Prevention & Online Authentication Market Guide 2017-2018

LATEST INSIGHTS INTO SECURING DIGITAL TRANSACTIONS AND COMMERCE

MRC Building Better Commerce
Fraud & Payments Professionals

HOLLAND FINTECH

As ecommerce fraud is constantly evolving and diversifying, the MRC relies on the annual Web Fraud Prevention & Online Authentication Market Guide to help thwart these challenges.

Danielle Nagao | CEO | MRC

Identity and authentication are becoming core to doing business online. This is necessary reading for everyone who deals with online customers and transactions.

Don Ginsel | Founder and CEO | Holland FinTech

THE PAYPERS

Web Fraud Prevention & Online Authentication Market Guide 2017-2018

LATEST INSIGHTS INTO SECURING DIGITAL TRANSACTIONS AND COMMERCE

Contact us

For inquiries on editorial opportunities please contact:

Email: **editor@thepaypers.com**

To subscribe to our newsletters, click **here**

For general advertising information, contact:

Mihaela Mihaila

Email: **mihaela@thepaypers.com**

RELEASE VERSION 1.0

DECEMBER 2017

TEL: +31 20 893 4315

FAX: +31 20 658 0671

MAIL: EDITOR@THEPAYPERS.COM

Editor's letter

The fundamental shift from physical cards, checks, and currency to digital payments continues to transform the way consumers and businesses transfer value. Identity, security, and trust are fundamental to payments, commerce, and finance, especially in an increasingly digital economy. The battle against cyber criminals is real and ongoing. Technologies like tokenization, biometrics, AI, and machine learning are helping to authenticate customers, secure transactions, and mitigate fraud loses. With this in mind, fraud prevention services providers, retailers, PSPs, and policy makers have started to develop advanced fraud prevention solutions and establish a legal framework in order to keep fraudsters at bay and maintain sensitive data secure. Featuring a three-part structure, our 6th edition of the **Web Fraud Prevention and Online Authentication Market Guide** provides payment and fraud and risk management professionals with a series of insightful perspectives from industry associations and leading market players on key aspects of the global digital identity transactional and web fraud detection space.

Fraud detection and prevention – best practices

Users are increasingly comfortable with online, mobile, and in-app purchases, and they expect the ease of an in-store experience, regardless of the channel. Biometric authentication, device fingerprinting, and continuous fraud monitoring are allowing the introduction of new risk based authentication models to streamline the checkout process and reduce basket abandonment. **Fiona Brown, Markus Bergthaler** from **MRC**, **Ron van Wezel** from **Aite Group, Manoj Kheerbat** from **Gropay** share with us the new models, technologies and regulatory specifications that are making waves in the industry, and how we stay one step ahead of the fraudsters whilst meeting customer expectations for frictionless commerce.

Biometric authentication technology is likely to be a game-changer. Thanks to the widespread accessibility of mobile biometrics and an increasing demand for reliable antifraud measures, strong authentication is out in the world, changing the financial lives of users everywhere. We have included in our guide expert biometrics vendors such as **Easy Solutions**, and mobility security consultants and associations such as **FIDO Alliance** that discuss real deployments of biometrics in commerce, and the opportunities, challenges, and success stories therein.

With an increase amount of data flowing across ever blurring geographical boundaries, the question of how to tackle fraud across the community and beyond has been both difficult and increasingly important, agrees **Neira Jones** from **Emerging Payments Association**. Users' data is the new money, and technology has enabled new entrants to challenge incumbents by capitalising on that data to understand behaviours and appear more human.

From IBM's Watson to Amazon's Alexa, AI is stepping into every aspect of our lives. Nevertheless, while data can be a catalyst for improving customer experience, it also creates an exposure to vulnerabilities like new fraud patterns, massive fraud attacks, and data breaches. **Nuno Sebastiao** from **Feedzai** agrees that banks should turn to AI systems to help them navigate a complex set of broader goals: mitigating risk, remaining competitive, and offering cutting-edge customer experience. Furthermore, **Roberto Valerio**, **CEO Risk Ident** considers that businesses which combine the human element with machine learning and AI capabilities can scale their fraud protection system, allowing it to grow and evolve to changing threats.

If by now merchants are still not convinced by the machine learning capabilities, **CyberSource** shares with us two types of machine learning, static and self-learning, and the benefits associated with them, to enable businesses to take on fraudsters. In this world of ongoing data breaches, sophisticated phishing attacks, and personal data changing hands on the dark web, all financial institutions and ecommerce companies must come to terms with their risk of Account Take Over fraud. However, with the proper tools and guidance, **Kevin Lee** from **Sift Science** thinks that you can not only protect your business, but also build long-term brand loyalty.

The role of financial services in creating digital identities

The ubiquity of mobile devices and tremendous growth in connectivity is fundamentally changing the way that individuals bank and access other financial services. However, a key hurdle in this transformation is the issue of trust in online transactions. A robust digital identity platform is the linchpin to verifying and authenticating users not only to establish trust in online transactions, but also to secure customer trust. ➔

Emma Lindley from **Innovate Identity** invites us to think differently the Know Your Customer processes as many KYC systems are based on data like names, addresses, date of birth, which easily exposed by data breaches and launches a call for action for organisations to create user-centric identity schemes. Together with **Jon Shamah** from **EMMA**, she offers numerous examples of such eID schemes around the globe.

Over the past two decades, India has witnessed manifold growth – socially, economically and technologically- and part of this grown it is the creation of Aadhaar, a 12- digit number allocated to each Indian resident that stores their biometric and demographic data in a centralized data base. However, is Aadhaar IDs story a qualified success? **Anshuman Jaswal** from **Kapronasia** offers the pros and the cons of the story and lets us to decide.

As regtech is booming, many regtech solutions focus on digital onboarding, meeting Know Your Customer (KYC) and Anti-Money Laundering (AML) requirements and present significant benefits to consumers, businesses, and regulators alike. However, despite these shared benefits, the interests of consumers, businesses, and regulators do not always align, as KYC legislation is not harmonized in Europe. How can we better align the interests of consumers, FSPs, and regulators? To identify the pain points, **Erin Taylor** from **Holland FinTech** examines the relationships between these parties and the processes flow involved.

Nevertheless, a team of consultants from **Innopay** believes that this lack of harmonization could contain hidden benefits. Furthermore, they have developed an approach to turn regulatory requirements of AMLD4 into a competitive advantage and share it with us.

With regulation serving as almost an underlying "operating system" for financial services, it is critical for industry operators to understand how to navigate a regulatory landscape that is constantly evolving. Every mobile app, website or enrolment form asserts that "your privacy is important to us" followed by a vaguely worded legal language that is difficult for the average consumer to decipher. The laws and liability associated with privacy and data security are constantly changing and are different in the US versus Europe. This guide will provide an overview of the regulations coming into force in 2018 in Europe, trends and actionable insights to help businesses navigate the privacy landscape.

Edwin Jacobs from **Time.lex** presents GDPR in a nutshell: what the main obligations under the GDPR are; when the notification is needed; sanctions, etc.; and all you need to know to start preparing for GDPR compliance. Not only GDPR, but PSD2 will definitely enrich and support customer experience in Financial Services and make banking more of an equal playing field, **Anupam Majumdar** and **Paul Weiss** from **Accenture** consider.

Infographics

Many businesses and governments are finding that they must provide better digital experiences for their users and gather more information about the consumers who are using their services. In the last few years, Consumer Identity and Access Management (CIAM), a sub-genre of traditional Identity and Access Management (IAM), has emerged to meet these evolving business requirements. CIAM systems must be able to manage many millions of identities, and process potentially billions of logins and other transactions per day. **Rob van der Staaij** from **Innopay** offers an overview of the Consumer Identity and Access Management (CIAM) market, the role of Cloud access security brokers (CASBs) and the dynamics that take place in this space.

To enable industry players to gain access to valuable information regarding the current Consumer Identity and Access Management providers landscape, we have created an explanatory infographic that highlights the main players in this field, together with identity verification, derived identification, and ID document verification vendors. Since last year's edition of the Web Fraud Prevention and Online Authentication Market Guide was accompanied by an infographic on Fraud Management, Authentication, and End-Point Protection, we considered that this year's edition should continue this good practice. Therefore, we have put together a second infographic which includes different solution providers in the ecosystem of Fraud Management.

We would like to express our appreciation to the Merchant Risk Council and Holland Fintech – our endorsement partners who have constantly supported us – and also to our thought leaders, participating organisations and top industry players that contributed to this edition, enriching it with valuable insights and, thus, joining us in our constant endeavour to depict an insightful picture of the industry.

Enjoy your reading!

Mirela Ciobanu
Senior Editor, The Paypers

Table of contents

Table of contents

Trends & Developments in Digital Banking and Ecommerce Fraud

The battle against cyber criminals is real and ongoing. Technologies like tokenization, biometrics, AI, and machine learning are helping to authenticate customers, secure transactions, and mitigate fraud loses.

General Overview of Fraud Risks in Digital Transactions

Everything Falls Apart Without Security – Key Trends and Developments

In their desire of growing a base of loyal customers, online businesses put a lot of effort in creating innovative products to ensure an excellent customer experience. Seamless checkouts and frictionless authentication – these are the two features that companies fight to consolidate and customers want to enjoy. However, ensuring protection is something that both online companies and consumers must take into account, although, this is not fully reflected in the customer experience, as security measures are implemented 'behind the scenes'. Online businesses need to provide security in order to gain consumers' trust.

There is a lot of buzz around digital innovation within the payments industry using blockchain, artificial intelligence and machine learning, robotic process automation, and mobile solutions, but as some of the experts involved in the online security environment say, it all falls apart without security. IT security and access management used to be regarded solely as an IT issue; a concern discussed only by experts in the field.

At the beginning of 2017, **Chris Skinner predicted** that:

1. RegTech moves deeper into bank infrastructure (and demands real-time access)
2. Regulators compete to innovate more (2016 bubbled, 2017 steams)
3. A major global bank gets broken into pieces (systemically important with systemic issues)
4. SWIFT gets hacked again (how many times can this happen?)
5. Machine learning and artificial intelligence are all the rage (related to above, but data wars begin)

Now look at what has happened: a major global bank gets broken into pieces (UniCredit Italy), SWIFT gets hacked again, the prolific use of biometrics (with the launch of iPhone x's Face ID, many banks now have adopted facial recognition for their mobile banking apps) increased number of data breaches (the biggest was the one affecting Equifax's customers), and ransomware attacks (WannaCry, Petya, BadRabbit); all the predictions came true. Today, terms such as 'hacking', 'ransomware', and 'data breach' commonly grab headlines in mainstream media: fraud is ever increasing in the new interconnected environments, and many companies are still unprepared for the consequences of large-scale fraud.

Therefore, taking into account that fraud detection and prevention, digital identity verification and consumer authentication are crucial in defining and securing the transactional ecosystem, special attention must be paid to these aspects. This part of the guide aims to portray what is currently happening in the fraud management, digital identity verification and authentication space. It also gives insights into the most common types of fraud that made the headlines in 2017 and offers best practices and advice on how to deal with them.

In this chapter, we will briefly discuss data breaches, chargebacks, card not present and CEO fraud, Account Takeover, and Transaction Laundering. You can find out more on how to act against these types of fraud and develop a strategy to prevent these from happening, while offering a seamless customer/users experience, by checking out further insights offered by payment and fraud professionals in the rest of the guide. →

Everything Falls Apart Without Security – Key Trends and Developments

Data breaches

Since 2009, more than seven billion online identities have been stolen in data breaches. Even more alarming is the fact that cybercriminals continue to target financial institutions and payments providers, and that the exploitation of data breaches and stolen identities has become automated, global, and coordinated.

Another day, another breach. Security experts have defined data breaches as security incidents that lead to the unintentional release of secure or private/confidential information to an untrusted environment. Data breaches may involve personal health information (PHI), personally identifiable information (PII), trade secrets, or intellectual property. The most common concept of a data breach is an attacker hacking into a corporate network to steal sensitive data.

According to the **Internet Security Threat Report from Symantec**, almost 40% of information lost in data breaches in 2016 was Personal Financial Information, which can include credit or debit card details or banking financial records. This figure increased by more than 6 % from 2015.

For 2017, the most notable data breaches occurred at Chipotle's, Verizon and Equifax, one of the largest credit agencies in the US.

During 2016, **Services was the most affected market segment** by data breaches, with almost 45% of breaches occurring in this sector, followed by the Finance, Insurance, and Real Estate at 22%.

The country most affected by data breaches was the United States, both in terms of number of breaches and the number of identities stolen. This is unsurprising, because the US has a large population, thus a high adoption of technology, and a large number of companies are based there. The first five countries most affected by data breaches are; the United States with 1023 breaches, United Kingdom with 38, Canada with 19, Australia with 15, India with 8.

In the first half of 2017, a significant number of data breaches were caused by accidental loss or exposure of data, including the improper erasure of records and inadequate database security. At a global level, there were 918 data breaches during the first half of 2017, compared with 815 in the last six months of 2016, a 13% increase. Of these, identity theft accounted for three quarters of data breaches, an increase of 49% compared to the previous six months. Finance companies have experienced a sad scenario: 5 million records have been stolen as a result of these attacks, accounting for less than 1% of the total, according to the **Breach Level Index** by Gemalto. The same report has revealed that the ecommerce industry, which is another common target for fraudsters, suffered 112 breaches. The records involved in the data breaches was rather low, at 4 million, which represents less than 1% of all lost, stolen or compromised records.

What is the cause?

Most of the time, data breaches are attributed to hacking or malware attacks. While these attacks play a big role, they only account for a quarter of all the reported incidents. Among top causes of data breaches in 2016 Symantec lists: theft of data, improper use of data, phishing, spoofing, social engineering, accidental data loss, loss or theft of device, IT errors leading to data loss, network disruption or DDoS attacks. →

Everything Falls Apart Without Security – Key Trends and Developments

What are the consequences?

The main risks associated with data breaches are the identity theft, which is also a common way of attack, followed by financial access and account access.

For consumers, data breaches mean identity theft, mostly. Identity data is the critical currency in global cybercrime, as fraudsters piece together full and convincing identities, which are then used to perpetrate large-scale attacks. Once compromised, fraudsters can make fraudulent purchases, manipulate listing information, create fake reviews, or change account information to divert pay-outs to their own bank account.

For businesses, security incidents could cost senior executives their jobs and have serious reputational, brand and business impacts. Under GDPR's 72-hour breach notification requirement, **institutions can receive financial penalties of up to 2% of the previous year's annual revenues for a first offence and 4% for repeat offences where the regulator has previously ordered remedial action**. There are also possible criminal penalties for executives deemed responsible, and consumers and affected third parties have the right to sue organisations responsible for data breaches.

According to **Kount's Mobile Payments & Fraud: 2017 Report**, merchants reported spikes in fraud following major data breaches and were most likely to be concerned with the brand damage following a security incident, as 44% of merchants said the most damaging aspect of suffering a data breach would be consumers perceiving them (the merchant) as having weak security. Moreover, merchants were very concerned with the loss of personal and financial data, considered the most damaging by about 34% of merchants.

Predictions

Even if data breaches seem to have grabbed headlines lately, security experts and companies continue surveying the ever-changing security landscape and assess their own preparedness for the worst. As attackers continue to sell old username and password information on the dark web, more companies will push toward using two-factor authentication to verify users. Secondary authentication methods could include tokens, SMS alerts, geo location confirmation, or biometrics.

All the breeches that took place in the restaurant and hospitality industry in 2017, where payment cards information was stolen using well-coordinated and expansive use of different types of Point-of-Sale (POS) skimmers, revealed that criminals continue to focus on payment-based attacks despite the EMV shift taking place over two years ago.
The Equifax example of how NOT to handle a data breach showed that businesses are relatively unprepared for such security incidents and these types of negative actions will cause big headaches for multinational companies. In particular, the General Data Protection Regulation (GDPR) in the EU will create more pressure for businesses and greater consumer awareness around breach notification and will lead to increased fines for companies/financial institutions that fail to comply with GDPR regarding the 72-hours data breach notification. →

Everything Falls Apart Without Security – Key Trends and Developments

Chargeback Fraud (Friendly Fraud)

What is chargeback fraud or friendly fraud?

There's nothing friendly about chargeback fraud. Chargeback fraud is often called friendly fraud because consumers fraudulently use the chargeback process to secure a refund. Chargebacks occur when customers contact their credit card issuers to dispute a card transaction and secure a refund for the purchase. They differ from traditional refunds because the consumer goes over the merchant's head and asks the bank to forcibly remove funds from the business's bank account, rather than contact the business for a refund. If the bank feels the cardholder's request is valid, the funds will be removed from the merchant's account and returned to the consumer. Thus, consumers illegitimately dispute a transaction with the bank instead of contacting the merchant for a refund.

They might claim the item was not delivered, or it was not as described or was defective, the original transaction was not authorized, or a recurring transaction was not cancelled as requested.

When introduced, in 1968 by the Truth in Lending Act, chargebacks were a form of consumer protection for credit card holders. However, they have since evolved into a weapon that consumers use against merchants. Friendly fraud is often called chargeback fraud because consumers use the chargeback process to steal from merchants.

The chargeback process

The customer, who is also the cardholder, disputes a transaction by contacting his/ her issuing bank. Depending on the cardholder's issuing bank, the process to dispute a transaction can be relatively quick or slightly more involved.

After the cardholder disputes a transaction, the issuing bank reviews the claim to determine whether or not the dispute should be sent to the card network. Once the issuing bank has determined the cardholder's dispute to be valid, an immediate credit is provided to the customer for the disputed amount.

While the issuing bank provides the credit to the cardholder, the card networks initiate the flow of funds from the merchant's commercial bank account back to the issuing bank. Once the customer is reimbursed, the issuing bank submits the chargeback to the card network. The card network then passes the chargeback to the acquiring bank.

After the acquiring bank is notified of the chargeback from the card network, it notifies the merchant of the dispute through a merchant account processor online portal or an offline letter by mail. Now that the merchant knows a chargeback has been filed, it is up to them to decide whether or not to submit a response.

Chargeback rules vary by card network. It is essential for merchants to carefully review each network's guidelines and regularly check for updates. Regulation manuals are updated twice a year (usually in April and October) with smaller changes being implemented continuously.

Reviewing the policies for each network is a tedious, time-consuming, and confusing process. These massive documents are filled with complex industry jargon and assumed credit card intelligence. →

Everything Falls Apart Without Security – Key Trends and Developments

How chargebacks affect merchants

Each time a consumer files a chargeback, the merchant has to pay a fee that can range from EUR 17 to EUR 112 per transaction. Even if the consumer later cancels the chargeback, the merchant will still have to pay the administrative costs associated with the process.

The Fraud Report 2017 by Worldpay has revealed that for several merchants, chargebacks fraud represented the majority of their fraud – 60% in one case. This issue is also a matter of circumstances. For example, within the US travel and airline sectors, fraud prevention experts expect a high rate of chargebacks fraud due to the weather incidents, because people quit the flight, although the flight was not cancelled, and claim a refund. However, few merchants seek a chargeback reversal. **Statistics** from The Chargeback Company show that 28% of merchants contest all chargebacks, 42% of merchants contest less than half of all chargebacks, and 14% of merchants never contest chargebacks.

Moreover, if monthly chargeback rates exceed a predetermined threshold, increased fines will be imposed upon the business. Businesses that experience significant chargebacks might be forced to obtain high-risk merchant accounts. These accounts come with steep processing fees and revenue-stealing rolling reserves.

How chargebacks affect consumers

Considering the definition of chargebacks, it might seem like merchants are the only individuals who can be victimised by illegitimate chargebacks and friendly fraud. In reality, both the merchant and the consumer suffer.

If a consumer files a chargeback and the bank discovers it is a case of friendly fraud, the card account can be closed, and the consumer might have to pay the accompanying chargeback fees for illegitimate chargeback disputes. Moreover, losing a card account can negatively influence a consumer's credit score.

Furthermore, in an effort to compensate for predictable chargeback fraud, merchants are raising their prices.

Responsibility

Retail fraud continues to rise dramatically, as does its cost. By taking the necessary steps to detect fraud, merchants can identify transactions that could potentially lead to chargebacks, both legitimate and illegitimate, and reduce their occurring risk.

Card Not Present Fraud

What is it?

Whenever customers purchase an app on their phone, a song on iTunes, or clothes from their favourite website, they are conducting a card not present transaction, as the cardholder does not physically present the card to the merchant. It can include telephone, Internet, and mail order transactions. Generally, the payment card information that is used in this process includes: the card number printed across the front of the card, the card's expiration date, the card security code and personal billing information. ➔

Everything Falls Apart Without Security – Key Trends and Developments

Card present transactions have become difficult to compromise, so fraudsters have started to exploit the online payment environment, with ecommerce as a specific target. The ecommerce sector has registered growing numbers of cases in over half of the European countries. According to the **Internet Organised Crime Threat Assessment by European Cybercrime centre**, non-cash payments are constantly at risk, as fraudsters perceive the online transactions space as a goldmine. CNP transactions are usually at risk because the process does not involve an interaction with the merchant, therefore, the fraudster can easily take advantage of this. The Merchant Risk Council (MRC) conducts an annual study to analyse the state of CNP fraud globally and discover what fraud prevention solutions are being used by participants in the payments ecosystem. According to the **2017 Merchant Risk Council (MRC) Global Fraud Survey**, MRC merchants reported that the type of fraud attack they experienced most frequently was clean fraud, in which fraudsters use stolen credit card information and other customer information to make purchases.

As the number of ecommerce transactions continues to grow, so does CNP fraud; **in Europe ecommerce is set to increase by 19% during 2017** and in Brazil, Russia, India, China and South Africa ecommerce will become a thriving industry with an increase of **340% by 2020, at which point it will have reached USD 3 trillion in BRICS countries**. Past experience suggests that CNP fraud will follow suit and become bigger than ever.

How do we identify (CNP) fraud?

Certain behaviours can indicate that a transaction has a higher risk of being fraudulent. Issues related to product / orders could include larger-than-normal orders or multiple orders for the same product. Also, the purchase of multiple same items could indicate that the customer intends to resell the goods on eBay or elsewhere to obtain cash. Other red flags for card not present fraud may be usage of multiple cards for a single purchase, orders for products readily convertible to cash (gift cards), orders made up of “big-ticket” items.

In terms of delivery, fraudulent customer requests “rush” or “overnight” delivery, a single card is used with multiple shipping addresses, delivery is done to an international address and the billing address is different from the shipping address.

Other red flags may be that orders have different names, addresses, and card numbers, but are from a single IP address, Internet addresses at free e-mail services, multiple transactions on a single card over a short time period, and a first-time customer with an order that does not fit the “average” customer purchase pattern.

Liability

If a fraudulent CNP transaction is reported, the acquiring bank hosting the merchant account that received the money from the fraudulent transaction must make restitution; whereas with a swiped (card present) transaction, the issuer of the card is liable for restitution. →

Everything Falls Apart Without Security – Key Trends and Developments

When CNP fraud occurs, the merchant bears the loss. This type of fraud can have a significant impact on the merchant's **bottom line**, especially for retailers, which tend to have small **profit margins**. By contrast, in card-present fraud, the credit card issuer usually bears the loss, not the merchant. Under credit card terms and conditions, the credit card issuer will not hold the cardholder liable for any fraudulent charges, whether through card-present or card not present fraud.

Trends

Currently the US accounts for 47% of the world's card fraud despite that it represents only 24% of total worldwide card volume. Card-not-present transactions account for nearly 17% of all transactions, and is expected to reach 25% by 2018, according to **Cayan**, a payment technology company. **The European Fraud Map**, which is based on data from Euromonitor International and UK Cards Association, reveals that card-not-present fraud in Europe increased from 50% in 2008 to 70% in 2016 of the gross fraud losses.

Furthermore, the digital identity service provider ThreatMetrix, which tracks cybercrime quarterly, reported in its **Q1 2017 report** that attacks outpaced overall transactions by 50%, demonstrating the high-risk levels associated with the people's habit of buying things on phones and laptops. Mobile transactions grew 400% in the last two years, primarily driven by the increase in financial services account logins as users embraced the ease and convenience of mobile banking apps.

Over 53% of accounts come from mobile, showing how retailers are focusing on building relationships with their customers in the mobile space, prioritizing mobile sign-up and login procedures. However, this makes it easier for the fraudsters to conduct card-not-present fraud by obtaining card details through skimming, hacking, email phishing campaigns, telephone solicitations, or other methods.

Experts say the uptick in CNP fraud means that online authentication practices have to improve, and ecommerce retailers, like all merchants, **must move toward payment-card tokenization**.

Online retailers also need to invest in real-time fraud monitoring and behavioural analytics so that they can review buying trends and patterns across all channels, whether online or in-store.

CEO fraud

Also known as Business Email Compromise (BEC), CEO fraud has ruined the careers of many executives and has victimised more than 22,000 organizations worldwide.

Definition

FBI's Internet Crime Complaint Centre (IC3) **defines Business Email Compromise (BEC)** as a sophisticated scam targeting businesses working with foreign suppliers and/or businesses who regularly perform wire transfer payments. CEO fraud in particularly is a fraudulent action in which cybercriminals spoof company email accounts and impersonate executives to try and fool an employee in accounting or HR departments into executing unauthorised wire transfers, or sending out confidential tax information. →

Everything Falls Apart Without Security – Key Trends and Developments

Statistics

According to new figures from the FBI's IC3, online extortion, tech support scams, and phishing attacks that spoof the boss were among the costliest cyber scams reported by consumers and businesses in 2016. The complaint centre received slightly more than 12,000 complaints about CEO fraud attacks in 2016, totalling more than USD 360 million losses from this type of fraud.

Nevertheless, according to security experts, **FBI's ransomware numbers could be seen as too low compared to those happening in the real world**, because relatively few victims are reporting cyber fraud to federal investigators. →

Attack methods

To prevent this type of crime, understanding the different attack methods is key. One attack method is phishing. Phishing emails are sent to large numbers of users simultaneously in an attempt to "fish" sensitive information by posing as reputable sources. Banks, credit card providers, delivery firms, law enforcement, and tax agencies are a few common ones.

When the fraud activity is more focused, this means that the cybercriminal either studied the targeted group or gleaned data from social media sites to con users. This method is called spear phishing.
Fraudsters become bold and target top executives and administrators, typically to siphon off money from accounts or steal confidential data, an action that is called executive whaling.

Trends

Still, of all attack channels, email remains the most commonly exploited and spear phishing is the most prevalent form of attack. Malicious emails continue to easily bypass legacy spam filters, firewalls, and gateway security scans, with CEOs being spoofed the most.

Technology, while continuously advancing in intelligence, still requires a human touch. Machine-human collaboration is the only way to implement meaningful change to preventing the scourge of email phishing attacks that propagate the majority of hacks.

Account takeover fraud

In 2017, **account takeover fraud replaced** stolen financials as the fastest growing fraud threat for ecommerce websites and rose by an alarming 45% from 2016, putting online retailers at a loss of USD 3.3 billion dollars.
Unlike mass-registered fake accounts, ATO attacks are very harmful, as they target accounts created by real users. They contain valuable information such as financial data, and their activities are less likely to raise the suspicion of security solutions. →

Everything Falls Apart Without Security – Key Trends and Developments

What is ATO?

Account takeover (ATO) is a type of identity theft in which a fraudster steals a business's or individual's valid account information (such as credit card number) to access products and services using those existing accounts. It can also mean extracting funds from a person's bank account. This type of fraud is strongly connected to data breaches, for example, account takeover attacks had begun rising sharply months before the Equifax data breach was notified. The unauthorised access to an account seems to be a preferred method for fraudsters, rather than stealing data.

How fraudsters are getting access to users' accounts?

Methods used by criminal entities to obtain access to legitimate banking credentials of business and consumer accounts include: mimicking a financial institution's website, using malware and viruses to compromise a system to gain account access, or using social engineering to incentivise consumers or employees into revealing security credentials or other sensitive data. Social engineering can come in many forms and is not as easily recognisable as it was before. Fraudsters may initiate contact by email, phone calls, faxes, or letters in the mail in their effort to receive sensitive information.

Collecting the data

Hackers can collect large numbers of credentials, by either taking over legitimate websites already trusted by users, stealing the information shared by users with the trusted site, or establishing fraudulent websites for the explicit purpose of gathering credentials. Afterwards, they often use bots or credential stuffing tools to test stolen credentials as quickly as possible.

Criminals have also started to build apps pretending to be the legitimate ones for smartphones, or from a certain company, but they are really imposter apps, created for stealing account credentials.

Trends

Consumer accounts are an attractive target to fraudsters. Attacks on corporate accounts remain a constant threat, but criminal entities are broadening even more their search for targets to include consumer accounts. Lower value consumer accounts are targeted because individual accounts often do not have the same protections and levels of security regularly applied to business accounts.

Account takeover fraud is on the rise, caused by massive data breaches. In the wake of recent massive data breaches, such as the Equifax hack, a flood of stolen data is leading to a whole new wave of account takeover crimes. This trend is unlikely to come to an end any time soon. Deloitte, Sonic, Whole Foods, and even the US Securities and Exchange Commission (SEC) have suffered similar experiences in data breaches of unknown severity. Based on the number of data breaches that took place in 2017, it is likely that the stolen credentials will be used heavily toward ATO attacks in 2018.

Therefore, it is crucial that users and businesses to choose good passwords; account takeover is a process, however it is far less difficult when consumers insist on using the same password everywhere. →

Everything Falls Apart Without Security – Key Trends and Developments

Account takeover is bound to turn into device take over. Attacks coming through fake mobile apps and those that phish for credentials from your device have increased in numbers. This is enhanced by the fact that the mobile device and the phone number are becoming the standard second-factor in authentication.

However, advanced security features, such as biometric authentication devices, are being built directly into the smartphones that consumers use every day, giving companies new tools in the fight against fraudsters.

Transaction laundering merchant fraud

Transaction laundering, also known as credit card laundering or factoring, is a serious problem for the payments industry. The phenomenon occurs when legitimate merchant accounts are used to process unknown transactions for another line of business, be they illegal or otherwise.

In online sales, **transaction laundering tops USD 200 billion a year** in the US alone, of which at least USD 6 billion involves some type of illicit goods or services, sold by nearly 335,000 unregistered merchants.

Because transactions may come from a variety of different sources (shopping carts, payment pages, virtual terminals, etc.), are made with different payment methods (credit cards, digital currency, e-wallets), or are processed through a page that the acquirer may or may not have visibility of, transaction laundering is difficult to detect and prevent.

What are the fraudster's methods?

The tactics used by transaction launderers typically include using alternative payment networks, bank payments or are relying on cryptocurrencies. Using the dark web for refuge, payment hustlers can freely conduct illegal commerce as well as lurk and browse undetected to find the illicit products or services they are looking to buy or sell.

Another reason these criminals are able to operate online without being shut down is the fact that sometimes the victims themselves are using websites to purchase illicit products and services. In those cases, reporting the fraud to authorities would only bring about more questions on the illegal purchases.

According to G2 Web Services, the three most common types of transaction laundering are:

- Benign: Two legitimate businesses are sharing the same payment gateway;
- Malicious: An illicit business is sending transactions through a legitimate or shell account;
- Affiliate: An illicit business takes payment info, creates an affiliate account at a third party merchant site, and purchases goods to collect affiliate revenue.

Unfortunately for consumers and businesses, these crimes are not always a top priority or even on the radar of regulators and authorities. Sometimes, managed service providers (MSPs) do not investigate the real origin of transactions until they face sanctions or fines by credit card brands. National governments have put in place sets of procedures, laws, and regulations designed to stop the practice of generating income through illegal actions, also known as Anti Money Laundering (AML). ➔

Everything Falls Apart Without Security – Key Trends and Developments

Nevertheless, many AML efforts are often wrongly focussed on high-risk, high-volume merchants, while transaction laundering can happen also in multiple smaller-scale, seemingly low-risk players.

Many covered financial institutions already collect some beneficial ownership information and have updated their AML policies and procedures in anticipation of the Customer Due Diligence (CDD) Rule. As a matter of course, all covered financial institutions should revisit their policies, procedures, and training materials to ensure their current practices meet the requirements of the CDD Rule by May 2018.

Synthetic Identity Fraud (SIF)

This is a type of fraud that combines stolen data and fake information to create a new identity for opening fraudulent accounts and making fraudulent transactions. Financial institutions, including banks, are mainly affected by this trend, which also represents a major source of losses for financial institutions.

Synthetic Identity Fraud is a growing fraud trend and a particular type of scam commonly used in the US, which costs companies USD 50 billion per year. This estimation worries 70% of companies, including financial institutions, according to a **white paper** published by Idology. While banks encouraged merchants to install the chip readers needed to adopt EMV, they also smoothed the path for synthetic fraud losses. Companies are still struggling to identify and classify SIF, and for this reason it's difficult to assess the problem in an accurate manner. Consequently, companies include the resulting fraud in their general losses. Synthetic identity fraud may also be perceived as a consequence of data breaches, as well-versed fraudsters in creating fake identities need as much data as possible in order to generate a genuine-like digital identity.

Final remarks

Fraudsters never sleep and companies keep making the same mistakes and not properly investing in security practices, thus failing in creating a reliable risk assessment. It may seem that security breaches are bound to happen, however, the human error is the main factor facilitating the process of data leakage.

Retail fraud continues to rise dramatically, as does its cost. As merchants realised the potential of mobile commerce, they expanded their mobile channels. Fraudsters did the same with their techniques, and currently, the mobile environment puts merchants at risk, just as the online space does. Mobile fraud is likely to grow, and this means fraud cost as a percentage of revenues will be higher for merchants using mobile channels as well. This looks like a sad scenario, as merchants would become sceptical with mobile transactions and this may lead to a higher rate of false positives.

Overall, when figures run into billions, it means that the online space is still open to attack. Online businesses need new and tailored solutions in order to tackle the current fraud trends and stay ahead of the fraudsters' plans, while keeping an eye on the predictions revealed by security researchers.

Emailage

Synthetic ID Fraud: An Introduction

In the past, synthetic ID fraud was the tactic of consumers with poor credit ratings. Back then, it was also known as a "credit bust out" and the process consisted in opening credit card accounts or applying for loans, then default and move on. Now, fraudsters have discovered the same tactics, and are using them at scale to cause major headaches in almost every industry.

Synthetic identity fraud occurs when fraudsters use a blend of real and fake information to create a new "individual." In some cases, the information used is entirely false. The bad guys then will open up new credit cards or auto loans under the fake individual's name, with the goal of creating credit records and boosting the credit profile. In other cases, fraudsters will also make major purchases and even obtain driver's licenses and passports.

Why has it become the new go-to tactic for fraudsters?

"There is no "victim" in Synthetic ID Fraud. There is no real person to make a complaint. It takes a bit more time for a fraudster to create the ID but it has a much bigger payoff" -- Brett "Gollumfun" Johnson, former Cyber Criminal

The shift to EMV has pushed fraudsters to card-not-present fraud and new application fraud, which is directly correlated to synthetic ID fraud. Fraudsters only need minimal "true" information to commit synthetic ID theft. The appeal is that fraudsters don't need to have someone's entire personal information; they can simply synthesize it.

Synthetic identity fraud relies on the use of an identity that has been created in one of three ways:

- Pair a legitimate social security number (SSN) with a fake name
- Use an "inactive" social security number with a real name (typically a child or a deceased person)
- Completely fabricate both SSN and name

Creating a synthetic ID is not a very hard process, either. Due to large-scale data compromises, fraudsters have easy access to customer identities.

According to online fraud pioneer Brett Johnson, "A complete identity profile of a specific victim is sold on cybercrime forums and DarkNet marketplaces every day for as low as USD 10."

What's worse, there are ways to speed up this process. Fraudsters will now "piggyback" onto a legitimate cardholder's account as an authorized user. How is this accomplished? The tactics are very similar to those used on social media to convince people to deposit bad checks or receive a fraudulent wire transfer.

Today: a clear and present threat

This shift requires a more sophisticated approach to predicting and assessing risk, and so does prevention. The growth of synthetic ID fraud shows few signs of slowing down. Easy access to data that fraudsters use to create synthetic IDs will continue to make fraud an attractive option. **Javelin Strategy & Research** estimated that new-account fraud will soar 44% between 2014 and 2018, rising from USD 5 billion in annual losses to a projected USD 8 billion. →

Amador Testa

Chief Product Officer
Emailage

About Amador Testa: Amador Testa has nearly 20 years' experience on leading product management and strategy. He is an industry expert in online fraud, identity theft mitigation and cybercrime investigations. Amador has led global initiatives to mitigate fraud and improve customer experience in over 26 countries.

About Emailage: Emailage, founded in 2012 and with offices in Phoenix, London and Sao Paulo, is a leader in helping companies significantly reduce online fraud. Through key partnerships, proprietary data, and machine-learning technology, Emailage builds a multi-dimensional profile associated with a customer's email address and renders a predictive risk score.

www.emailage.com

Click here for the company profile

Share this story

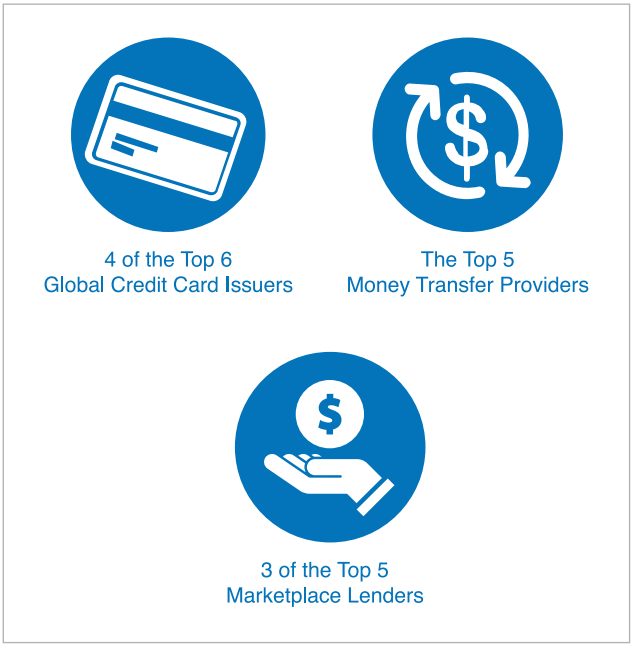
emailage®
The Global Hub of Email Intelligence

Here's how to fight back

There's one key piece that fraudsters need to successfully commit synthetic ID fraud: an email address. That's where Emailage comes in. To identify potential synthetic IDs, we use crowdsourced network intelligence to look for behaviour changes around the use of the email address in transactions.

Our predictive online fraud risk scoring uses email address meta-data as the core for transactional risk assessment and identity validation. Our online identity profiles fuse this data with other elements, such as phone number, address and customer name.

We help combat synthetic ID fraud by delivering insights that detect linkages and suspicious patterns, which help determine that the applicant is a real person. We also have a very strong network, with members that report suspected events associated with an email. Our network includes: 4 of the top 6 global credit card issuers, the top 5 global money transfer providers and 3 of the top 5 marketplace lenders.



Sift Science

Account Takeover – Protecting Your Business from a Growing Threat

If we have learned anything from the evolution of fraud, it is that fraudsters adapt. As soon as one point of attack is shut down, they find another way in.

We have seen this with the migration of "traditional" credit card fraud to card-not-present fraud, because the introduction of EMV made it harder for fraudsters to counterfeit physical cards. And now we are seeing criminals move from leveraging credit cards to leveraging stolen credentials and personal data to commit account takeover (ATO).

Why fraudsters flock to ATO

ATO – when a bad actor gets access to a good user's account – can be more profitable than credit card fraud. For one thing, many businesses do not have a robust solution in place for stopping ATO, so the window of time for exploiting the information before detection is typically longer. Furthermore, a credit card can only be used until it's cancelled. But even once an ATO is discovered, the fraudster still has access to the credentials or personal information, which can be used to create a new fake account or a synthetic identity.

ATO also provides fraudsters with the advantage of built-in trust. New accounts are more likely to be flagged for fraud or given more scrutiny. If the account already exists and is connected to a trusted user, you may give them more leeway and the fraudster has more time to operate before they are discovered.

Data breaches: Equifax and beyond

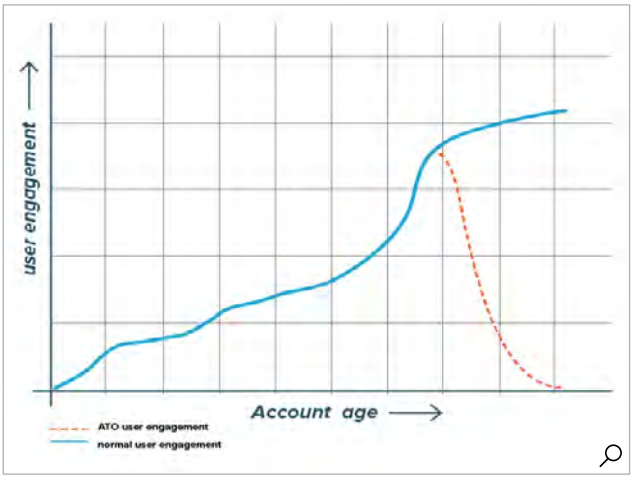
One major reason ATO is on the rise is the prevalence of large-scale data breaches, which provide a trove of personal information that can be mined for years to come. The Equifax breach – which exposed the sensitive information of nearly 700,000 Britons and 145 million Americans – was only the latest to affect consumers and businesses around the world. From Tesco Bank and O2 to Yahoo and eBay, breaches are increasingly becoming a global regularity.

The bottom line is that financial institutions and merchants across the world are going to be dealing with the effects of these large-scale breaches for years to come. It is easier than ever before for criminals to take over and exploit good users' accounts, as well as create synthetic identities using disparate pieces of information.

Measuring the impact of ATO

In terms of customer trust lost and brand damage, ATO can be a nightmare for companies. Collectively, victims spent 20.7 million hours resolving ATOs in 2016, according to data from **Javelin Strategy & Research**. While ATO may be harder to quantify than payment fraud, it can still be measured. You can start by collecting active inputs, every complaint and ATO reported to the Customer Support team. Then, you can try to gauge the number of unreported cases by analysing all of the users who have deactivated their accounts and trying to determine which ones were ATO victims.

After you gather these two sets of information, you can compare the long-term value of an affected user to that of a normal user (see graph below).



Kevin Lee

Trust & Safety Architect
Sift Science

About Kevin Lee: Kevin Lee is the Trust & Safety Architect at Sift Science. Prior to that, he led trust and safety, risk, chargeback, and spam teams at Facebook, Square, and Google.

About Sift Science: Thousands of global businesses depend on the Sift Science Digital Trust Platform to determine in real time which users they can trust. Sift Science's Live Machine Learning, global trust network, and automation technologies fuel growth while protecting businesses and their customers from all vectors of fraud and abuse.

www.siftscience.com

Click here for the company profile

Share this story

sift science
Move at the speed of trust

How companies can prevent ATO

To effectively protect your users from ATO, you must look at a range of relevant data points. Many signs of ATO are contained in subtle behavioural patterns across all of a user's activity. An effective solution can synthesise a range of activity and detect anomalies.

Some of the signals that may indicate ATO include login attempts from different devices, switching to older browsers and operating systems, changing settings and passwords, multiple failed login attempts, and suspicious device configurations – like proxy or VPN setups.

However, it's important to remember that each of these signs may be normal behaviour for a particular user. It's only when you apply behavioural analysis on a large scale, looking at all of a user's activity and the activity of users across the network, that you can get an accurate picture of whether a login is legitimate.

In this world of ongoing data breaches, sophisticated phishing attacks, and personal data changing hands on the dark web, all financial institutions and ecommerce companies must come to terms with their risk of ATO. With the proper tools and guidance, you can not only protect your business, but also build long-term brand loyalty.

ThreatMetrix

Ubiquitous Data Breaches Fuel Global, Organized Cyberattacks

Data breaches have become a painful, but regular, fact of life. Estimates continue to grow around how many billions of users have had their personal credentials stolen, while businesses scramble to reassure the consumer population that their sensitive payment details and encrypted passwords are safe.

Sadly, this widely misses the mark. What is evident through analysis of the ThreatMetrix Identity Abuse Index is that cyber-criminals are piecing together the jigsaw pieces of identity data (via advanced social engineering, phishing, data bought/traded on the dark web, and stolen via breaches) to create near-perfect simulacrums which are then used in global attacks. Individual pieces of identity data, no matter how apparently insignificant, are being pieced together to perpetrate highly organized and successful attacks.

ThreatMetrix Identity Abuse Index, 2017. An Identity Abuse Index level of High (shown in red) represents an attack rate of two standard deviations from the medium-term trend. Aggregated over all global transactions, this shows that the exploitation of stolen identity information is automated, global and coordinated.

What has become more and more evident in 2017 is that stolen identity data has an almost instant impact on attacks that we see in the Network. Fraudsters capitalize on the new blood of fresh credentials, acting fast with mass identity testing bot attacks, using validated credentials to takeover trusted user accounts, open fraudulent new ones, and make a vast swathe of bad payments with stolen credit card data.

We see this particularly clearly when we correlate the breaches we hear about in the news, with the attack patterns and key spikes in attacks that we see in the ThreatMetrix Identity Abuse Index. It's no coincidence that the highest attack volumes occur right after the most high-profile breaches; after all, the most valuable time for fraudsters is right after a breach has happened but before it has been discovered and reported.

It makes us ask the question, what constitutes an identity in the age of digital commerce? Are we who our username and password say we are, or are we built from the complex way we interact and behave online? How do our online selves merge with our offline ones? Is someone else using our image, name or email address? Who owns this identity? The challenge for many digital businesses is that they are trying to solve the problem of individual use cases in silos, plugging one gap while others remain vulnerable. At the same time, without a holistic view of your end user across their entire customer journey, it becomes impossible to validate their identity at each touchpoint.

A heightened threat landscape

With 171 million cyberattacks detected and blocked in Q3 2017, an increase of 32% just since the start of the year, cybercrime continues to present a growing and omnipresent threat to global digital businesses. There is strong impetus for organizations to orientate their strategy around preventing attacks, while minimizing the impact on existing, loyal customers. After all, a robust cybercrime defence is virtually useless if it creates a barrier to doing business, or makes users defect to a competitor because they are fed up with an online experience marred by friction, unnecessary step-up authentication and unauthorized transactions.

Businesses are being forced to look beyond traditional authentication methods to find a more holistic, layered approach to establishing true identity. The key imperative for ThreatMetrix is how to detect cybercriminals without increasing friction for legitimate users. We believe it is this dynamic that leads to strong brand reputation, customer loyalty and lifetime value.

Cybercrime outlook for 2018

Taking into account the nuances of this fast-evolving landscape of cybercrime in 2017, the outlook for 2018 looks equally challenging:

'1-Click' ecommerce will re-orientate payments landscape

With Amazon's patent on 1-Click commerce now expired, online retailers will manage to accelerate checkout speeds significantly. →

Reed Taussig

President & CEO
ThreatMetrix

About Reed Taussig: Reed Taussig is President & CEO of ThreatMetrix. With expertise in building high-growth companies at the forefront of technological change, Taussig has led ThreatMetrix since 2008. Under his leadership the company has become the driving force in an emerging digital identity space by leveraging pioneering global shared intelligence technology.

About ThreatMetrix: ThreatMetrix®, The Digital Identity Company®, empowers the global economy to grow profitably and securely without compromise. With deep insight into 1.4 billion anonymized user identities, ThreatMetrix ID™ delivers the intelligence behind 75 million daily authentication and trust decisions to differentiate legitimate customers from fraudsters in real time.

www.threatmetrix.com

Click here for the company profile

Share this story

ThreatMetrix
The Digital Identity Company

But, ecommerce players will need to carefully balance friction and fraud to achieve optimal ROI – without turning away good customers.

Cyber fraud and financial crimes will continue to converge

ThreatMetrix has seen fraudulent new account creations in financial services up 240% in two years (Q3 2017); 2018 will see cyber fraud combine with traditional financial crimes, such as the use of "money mules." This may take the form of fraudsters using automated bot attacks to apply for fraudulent loans or hijack existing accounts then transferring money to other countries.

Digital-only and new industries will be prime targets

Among those expected to face issues next year: peer-to-peer and sharing-economy platforms. Fraudsters are capitalizing on new platforms by monetizing credentials between fake driver/rider accounts in ridesharing and creating fraudulent new accounts for phony loan applications that they never intend to repay. The digital-only model of many of these companies makes them particularly susceptible to fraud.

Vulnerable consumers make valuable targets

As online, and particularly mobile, banking continues to drive financial inclusion for the unbanked and underbanked population, cybercriminals will pounce on these fresh and potentially more vulnerable new consumers who are often less adept at spotting the clever nuances of social engineering and phishing attacks.

Emerging Payments Association

Cyber Security: Trends and Implications in Financial Services

Kronos, Invisible Man, Spy Dealer, Faketoken, Double Pulsar, Trickbot… It's ok if you thought this was a list of Hollywood block-busters! These are in fact banking Trojans that hit the headlines in recent past and the creativity of the researchers who named them must be commended!

Artificial intelligence and machine learning, useful tools for the bad guys as well?

Kronos was the first to appear in 2014 – cybercriminals have always targeted financial service institutions, because, well, that's where the money is. However, the threat landscape has changed considerably in the last few years. The staggering advances in new technologies have made it possible to change the world for the better, with applications of artificial intelligence and the Internet of Things facilitating, for example, further financial inclusion and providing even better consumer experiences. However, this is a double-edge sword as technology has also enabled criminals and fraudsters to become even more innovative.

"Cyber" is now the tool of choice for financial crime as it makes it easier to swipe millions from financial institutions within seconds and dispose of the stolen assets quickly. Indeed, cybercriminals are starting to use machine learning to sift through large amounts of data to classify victims that have weaker defences, to maximise their return on investment, and conduct effective phishing campaigns on a massive scale.

Even more recently, fraudsters showed incredible nous by poisoning results for financial-related searches to **deliver banking malware** to unsuspecting consumers. In the UK, the National Cyber Security Centre has dealt with more than 600 "significant" cyberattacks since it was opened. In 2016, we saw the IoT harnessed to create the biggest ever DDoS attack, SWIFT members repeatedly hacked, and the scandalous leak of the Panama Papers. This was also the year when UK cybercrime figures were for the first time included in overall fraud figures, showing a 55% year-on-year increase, a fact that security and fraud professionals had always suspected. The 2017 is proving to be no different, and we only have to look at the massive Equifax data breach and the recent Paradise Papers leak, which brings into question the issue of data protection and privacy and how we manage digital identities.

How to harmonise and protect consumers' personal data?

With an increase amount of data flowing across ever blurring geographical boundaries, the question of how to tackle fraud across the community and beyond has been both difficult and increasingly important. In this complex landscape, protecting that data is a challenge that governments worldwide are trying to address in an attempt to strike the right balance between tech-nology innovation, competition, risk and security. Regulatory risk has never been so much in the limelight.

Governments have taken different approaches to financial services oversight. India's attempt to promote financial inclusion, with a universal digital identity scheme and fast demonetisation, has led to a boom in fintech innovation, but also created fraud/security risks which are now being addressed (in a recent move, the Indian Central Bank made the linking of national identity numbers – Aadhaar – to bank accounts mandatory). In China, technology giants Ant Financial (with Alipay) and Tencent (with WeChat Pay) have been quietly leading the mobile payments revolution. They achieved such a dominant position that not only has China's Central Bank ordered them to operate through a centralised clearing house (to promote competition), but has been worried that promotional activities might interfere with the normal currency flow of the CNY. China has also introduced numerous, and sometimes controversial, cyber security laws. As for the US, the fintech regulatory landscape is so confused that it is a wonder if any startup succeeds.

In the meantime, Europe brings in the 2nd Payment Services Directive (PSD2), the new Anti-Money Laundering Directive, the General Data Protection Regulation (GDPR), and many others. Unlike in any other geography, European regulations aim to be all encompassing at the outset. →

Neira Jones

Advisor and Ambassador
Emerging Payments Association

About Neira Jones: Neira advises organisations on payments, fintech, regtech, information security, regulations and digital innovation. She holds a number of Non-Executive Directorships and Advisory Board positions and is on the Thomsons Reuters UK's top 30 social influencers in risk, compliance and regtech 2017 and the Planet Compliance Top 50 RegTech Influencers 2017.

About Emerging Payments Association: The Emerging Payments Association (EPA) has over 120 members from across the payments value chain. We connect the payments ecosystem, encourage innovation and drive business growth, strengthening the payments industry to benefit all stakeholders. Get in touch at **info@emergingpayments.org** or +44 20 7378 9890.

www.emergingpayments.org

Share this story

In one fell swoop, these all intermingled regulations aim to protect and enable consumers (as in India) to foster technology innovation (as in China), and to preserve the integrity of the ecosystem (like everywhere). However, such laudable intentions also have their fair share of controversy, particularly for PSD2 and Open Banking.

Indeed, the EBA RTS on Strong Customer Authentication and Common and Secure Communications has set the cat amongst the pigeons: incumbents (i.e. the ASPSPs) love the stance on APIs and the ban on screen scraping, and the new kids on the block (i.e. AISPs and PISPs) loathe the ban on screen scraping as it may destroy their business model. And the debate goes on. Not to be left out, EMVco recently released the new EMV 3-D Secure Specification. All of these put digital identity and authentication firmly on the agenda.

Yes, Data (YOUR Data) is the new money (or oil, or coal), and technology has enabled new entrants to challenge incumbents by capitalising on that data to understand behaviours and appear more human. Unfortunately, the combination of data proliferation and technology advances has also created more risk. Fighting fraud and cybercrime effectively means being serious about information security and fraud prevention, managing the extended supply chain and understanding how new technologies can streamline operations (and the Regtech industry is currently flourishing...).

Regardless, the threat landscape is constantly evolving and many regulations will come into force in 2018. Organisations must be ready and their success will depend on their foresight, their risk management posture and how they capitalise on new technologies.

Merchant Payments Ecosystem

February 20-22, 2018 **Berlin**

REGISTER NOW TO SAVE 10%

Available until December 31

NEW FACES & NEW STORIES

150+ SPEAKERS

Fraud prevention innovators who:

Develop smarter customer authentication

Martin Sweeney, CEO, Ravelin
Ravelin imports a client's visitor, registration, and payment data in real time, via an API, inspects data using an AI, identifies and blocks fraudsters, and enables systems to prevent such crimes in future.

Automate identity verification

Stephen Ufford, CEO, Trulioo
Trulioo provides advanced analytics based on traditional information such as public records, credit files, and government data as well as alternative sources, including social login providers, ad networks, mobile applications, e-commerce websites, and social networks.

Merchant Payments Ecosystem (MPE)

THE European conference & exhibition on Merchant Payments Acceptance:

- Card Acquiring & Alternative Payments
- POS & Payment technology: online, mobile and in-store

Enable to on-board more customers with less drop-off

James O'Toole, Co-Founder & CEO, ID-Pal
ID-Pal's web portal (for the business) and app (for the customer) create a simple and effective system for capturing, verifying and storing customer ID documents and information.

Prevent chargeback fraud and minimise associated losses

Monica Eaton-Cardone, COO, The Chargeback Company
The Charback company prevents chargeback fraud and minimise associated losses by using proprietary technologies and machine learning, backed by expert human forensics.

1000+ ATTENDEES

40+ COUNTRIES

300+ C-LEVEL EXECS

70+ SPONSORS & EXHIBITORS

300+ FINTECH PEERS

Simplify merchant on-boarding

Christian Chmiel, CEO, Web Shield
Web Shield developed on-boarding hub that gathers all risk intelligence in one place and helping evaluate a merchant's viability through dynamically updated risk scores and indicators.

Request the agenda and register @ **www.merchantpaymentsecosystem.com**

Fighting Digital Banking and Ecommerce Fraud using Machine Learning and Artificial Intelligence

As fraud within online banking and ecommerce channels becomes more prevalent and damaging, Artificial Intelligence (AI) and machine learning promise to radically shift the balance of power between merchants and the criminals who seek to steal from them.

Feedzai

Key Considerations for Managing Digital Fraud at Speed and Scale

Consumers are increasingly seeking digital channels to transact, whether for shopping or opening a bank account. Open banking initiatives like PSD2 in Europe have been creating a competitive environment for banks, in which data has become the new currency. **According to PricewaterhouseCoopers**, in 2015, the year of the PSD2 release, the UK saw more electronic payments than cash payments for the first time. And in 2018, the year of its implementation, 20% of online transactions are likely to be made with mobile devices.

With the rise of digital commerce and the proliferation of new channels and payment types, data can be a catalyst for improving customer experience. On the other hand, data also creates an exposure to vulnerabilities like new fraud patterns, massive fraud attacks, and data breaches. The result of our growing digital economy is a steady increase of fraud across the globe. Global card fraud losses have nearly quadrupled since 2010, from USD 7 billion in 2010 to USD 27 billion in 2017, **according to The Nilson Report**.

One characteristic of today's fraud is the high financial loss. Beneath the money loss, there's everything else, from law penalties to operational disruption. Furthermore, every breach opens the door to new fraud activities, like account takeovers and massive fraud attacks.

But the costliest consequence of these crimes is that people get hurt. When someone has his identity or credit card information stolen, society suffers. Managing risk is rooted in a goal deeper than saving money. The goal is to make society safer.

To achieve this goal, organisations must deal with a key characteristic of today's fraud: its high velocity. Criminals deploy speed as a tool and leverage the most advanced technology to launch rapid attacks. For example, at Feedzai, we've discovered fraudsters using bots that fill forms five times faster than humans.

Banks have come to conclude that they need more sophisticated tools in order to detect fraud at scale and in sub-millisecond transaction time. Banks are turning to AI systems to help them navigate a complex set of broader goals: mitigating risk, remaining competitive, and offering cutting-edge customer experience. Here are three considerations to be taken in the pursuit of that machine learning system that can enable banks to stay ahead of new and evolving fraud.

Consideration 1: Refocus on the customer with a complete view

Because banks today are product-centric, rather than customer-centric, they make decisions in silos and are vulnerable to attacks across multiple channels for the same account. How can a bank know whether a customer defaulting on a credit card bill is a risky customer for a home mortgage?

Machine learning can break down data silos by performing omni-channel aggregation and omnidata integration. The result is a 360 degrees view of transactions right as they happen.

To build up a complete customer view at speed and scale, a machine learning system needs to be data agnostic, to be conceived for the purpose of extracting and loading all kinds of data, whether they are within the bank's own system or are augmented from external sources.

Consideration 2: React to fraud faster

With digital transformation comes the expectation of immediacy. Customers want decisions made at the speed of transactions. The increase of immediacy trends in payments, such as Amazon 1-click ordering, are only reducing the amount of time it takes for customers to transact.

To manage the risk associated with immediate transactions, banks need a system that can accelerate the machine learning process and lead fraud analysts and data scientists to fraud drivers more quickly. The benefits of speeding up the machine learning process are explored more deeply in the report **Improving Fraud Detection by Speeding Up Machine Learning**. →

Nuno Sebastiao

Co-founder and CEO
Feedzai

About Nuno Sebastiao: Nuno is co-founder and CEO of Feedzai, an agile machine learning platform for risk management. Previously, Nuno led the development of the European Space Agency Satellite Simulation Infrastructure, contributing to the Rosetta space probe. Today, Nuno and his team of top data scientists and experts in payments technology are working to achieve a singular mission: to make commerce safe.

About Feedzai: Feedzai is coding the future of our digital economy with the most advanced risk management platform, powered by big data and artificial intelligence. Some of the world's largest organisations use Feedzai's machine learning technology to manage the risk associated with banking and shopping, whether it's in person, online, or via mobile devices.

www.feedzai.com

Click here for the company profile

Share this story

feedzai

To enable organisations to react to fraud faster, a system must be also architected for the rapid deployment of new models. Furthermore, as analysts review transactions and label them as fraud or not, the platform should integrate with those decisions and automatically learn from them to become better at recognising future patterns.

Consideration 3: Pursue explainability

As more and more banks are turning to machine learning to make good decisions, they're realising the need for explanations too. Transparency and interpretability in a machine learning system have two important benefits.

First, a system with interpretable reasoning lets organisations audit the machine and provide trails of explanations for compliance. Second, better explanations means banks and merchants can drive greater engagement and deliver greater customer experience.

Today explainability exists in the form of whitebox processing, which adds human-readability to the underlying machine logic and communicates factors behind its decisions to the human analyst. What does the next stage of explainability look like?

What's next for machine learning?

My colleague, Pedro Bizarro, Feedzai co-founder and CSO, has said that the critical need for explainability calls for a machine that can link patterns with increasing complexity, and explain even more underlying connections to "what's actually going on."

The maturation of explainability will expose humans to more sensitive information, which raises questions around ethics. To reduce bias in AI, and to protect the integrity of enterprise data and the privacy of machine insights, Bizarro has developed an internal AI Code of Ethics, and he's asking AI practitioners to help shape the future of ethical machine learning. He explores this future in the report **What's Next for Machine Learning: Ethics and Explainability in AI for Fraud**.

Simility

Adaptable Fraud Prevention: Insights Across Banking Channels

The rapid adoption of mobile banking presents many opportunities for the financial services industry. However, fully embracing this digital transformation comes with numerous challenges—which require a fully adaptable approach.

It's not easy to add and maintain support for mobile and desktop users, yet alone build and preserve a competitive edge over multiple newcomers in the digital world. Thriving in mobile banking requires supporting technologies that are constantly changing and evolving, and there's pressure to add new services such as remote chat and video-based advisory amenities. Furthermore, consumers are demanding a faster and smoother process when creating new accounts and performing transactions, and that adds additional risks and complications.

Detecting fraud without adding user friction

Perhaps the biggest challenges to fully adopt mobile banking are the added security and fraud risks. The many technical complexities of digital banking introduce a whole new array of security vulnerabilities and their associated risks. Furthermore, opening the door to remote customers also opens the door to cybercriminals and fraudsters.

Adding layers of security is necessary, but it can have a negative impact on users. For instance, banks are faced with the dilemma of how to accurately validate the identity of remote individuals applying for new accounts or performing transactions—without annoying legitimate customers with a multitude of security questions and hurdles.

This task becomes even more difficult when multiple channels are involved. No financial service markets are exclusively digital—a personal, human touch will remain critical for years to come. That means banks must support in-person, fully-digital, and a hybrid of both types of banking. Consider a situation where a customer uses their mobile phone at night to begin a loan application, but finds it necessary to ask a few questions via the call centre the next day, and then finish the process in-person at the branch. For both the bank and the applicant to have a smooth and efficient experience, information from all three channels (the mobile app, the call centre, and on-site) need to be fully integrated. To quickly and effectively validate the identity and data provided by the applicant, the loan officer needs a consolidated view of data and risks from different sources, including:

- Data entered via the bank's mobile app
- Mobile phone fingerprints
- Device cross-checks with blacklists and whitelists
- User location
- Information gathered via the session with the call centre
- Data from the on-site application process
- Third party validation of the individual's name, address, and other personal data

Regardless of which channels are used, for a bank to evaluate and approve new accounts or any transaction, the bank must ingest data from multiple, disparate sources and quickly analyse, calculate, and present the risks so a decision can be made.

Omnichannel banking requires an adaptable fraud prevention solution

Today's banks not only need to gather fraud data from multiple, different and often incompatible sources, but this data is constantly changing—both in format and in source. Successful fraud mitigation must constantly adapt to varying amounts and types of unstructured data, evolving threats, and continuously-changing regulations and policies. This requires a system that is specifically designed to automatically adapt to this ever-changing environment.

The success of such an integrated and adaptable approach rests on four pillars:

1) Enriching the data lake with pertinent information to create a customer 360-degree view

Since the goal is to create a 360-degree view across products and channels, the fraud solution must ingest structured and unstructured data from any channel and user device—in real time, as well as, batch mode. It must be possible to gather data from home grown and third-party systems along with mainstream tools. Furthermore, the solution should include smart-ingest capabilities that simplify the incorporation of data from any source or format. →

Rahul Pangam

Co-Founder and CEO
Simility

About Rahul Pangam: Rahul Pangam is the Co-Founder and CEO of Simility. He's an industry veteran, with impressive experience from Google, who is dedicated to empowering fraud fighters with the most adaptable, scalable, and accurate fraud analytics platform.

About Simility:
Simility provides intelligent fraud prevention that grows with you. Our flexible platform ingests data sources in the public or private cloud or on site. Plus, you can easily bring in new sources (whether structured, unstructured, or data lakes) as you grow. Without having to write a single line of code, your analysts can quickly and accurately identify evolving fraudulent tactics across silos and create appropriate rules, thanks to a powerful combination of human intelligence with Simility's self-optimizing machine-learning models. Simility helps you spot and stop fraud in real time while providing greater fraud intelligence with fewer false positives.

simility.com

Click here for the company profile

Share this story

simility

2) Leveraging data analytics to build fraud indicator models
Banks have many areas where machine learning (ML) and data analytics can efficiently detect fraud. Superior fraud detection solutions can run multiple supervised and unsupervised ML models in parallel, each tuned for specific use cases such as account takeover, new account fraud, or payment transactions. This level of granular adaptability is necessary for a comprehensive and effective solution.

3) Insightful, visual dashboards and reporting
Efficient case analysis requires intuitive visualization tools that can provide fraud analysts with comprehensive and relevant data. For analysts to quickly adapt to evolving scenarios and make a decision regarding each transaction under review, the system must provide both summary and detailed information of all events.

4) Enabling continuous refinement and improvement with dynamic ontology
Finally, the solution should give omnichannel businesses the opportunity to set their own rules and configurations to manage fraud movement across multiple channels. This adaptable approach ensures that the fraud detection solution's performance continues to improve as the business evolves or as threats mutate. Also the addition of new data sources requires a flexible modelling capability that can evolve quickly to incorporate the new data sources.

Conclusion

To stay competitive in today's digital and omnichannel world, banks must increasingly use evolving technologies that contain vulnerabilities and increase the risk of fraud. Fortunately, there are tools to help mitigate the risks. Organizations in the financial services industry need to carefully evaluate fraud detection solutions they put in place. The choice solution must adapt to an ever-changing environment, be affordable to sustain, and effective at identifying and stopping fraud.

Risk Ident

Fraud prevention is not IT security. Of course, there are similarities between the two; you can never be 100% secure, both are a cat and mouse game – the harder you make it for the attackers, the less likely you are to be hit!

What's the relationship between fraud prevention and data breaches?

The two come together when fraud prevention is required to deal with the consequences of a data breach. Take, for example, the Equifax breach, one of the biggest data breach stories in 2017, which saw 140+ million credit records from US citizens placed in the hands of criminal organisations.

Fraudsters have, no doubt, already been using those details and will continue to use the stolen info in the months ahead, targeting online merchants with well-resourced account takeover (ATO) attempts.

> *"Fraudsters learn to exploit the weaknesses of traditional fraud prevention tools over time. It is crucial for businesses to combine human expertise and machine elements to prevent fraud.*

How does account takeover (ATO) fraud work?

ATO occurs when a fraudulent entity gains access to a legitimate account – with an online retailer, for example – then uses the account holder's details and stored payment information in order to pay for goods. The fraudster effectively hides behind the customer's good history, causing undetected havoc. By the time the customer, the retailer or the bank have raised the alarm, the damage is often already done, the goods are shipped and the transaction charged to the account.

Unfortunately for larger businesses, the bigger the company (merchants, mobile network operator, banks), the more likely fraudsters will find overlaps within their stolen data. Get inside the mind of a fraudster if you obtain stolen user credentials (which include e-mails and passwords) from the likes of Dropbox or LinkedIn, you're going to try out those credentials first at Amazon or Best Buy, not at a small online retailer.

How can customers play a more active role in fraud prevention?

Since fraud moved almost exclusively online, fraudsters have been able to play an enormous game of 'trial and error' that was never possible in the physical world. Once they have one set of online credentials, they test them across dozens of different online merchants in a matter of minutes.

It's therefore critical that consumers keep a varied range of passwords and security questions so that if one account is compromised, the rest will not fall like dominoes. However, the inconvenient truth is that customers have always been the weakest links in online security. A recent survey found **that 80% of consumers** reuse the same password across multiple accounts. With data leakages now reaching **'epidemic levels'**, it's clear that the industry needs far stronger communication on how to stay safe online.

For concerned consumers worried about security, there are software vendors out there that will manage your entire spectrum of passwords, like 1password or KeePass. If that is too technical for you, our advice is to keep a notebook of all your online passwords at your desk. Sure, the book could be stolen but it's far safer than limiting yourself to only one or two different passwords.

What can businesses do when they're struggling against weak password security?

ATOs aren't purely down to poor password discipline by end-consumers; passwords themselves are a flawed form of authentication. Two-factor authentication, asking users to provide an additional piece of information known only by them, in addition to passwords, is an important step forward in reducing the chances of ATO fraud. Merchants should also look at sealing leaks caused by outdated payment methods such as open invoicing. However, the most important step forward is to ensure that modern fraud is met by modern fraud prevention. →

Roberto Valerio

CEO
Risk Ident

About Roberto Valerio: Roberto Valerio is one of the foremost experts on the rise of AI in combating fraud, and founder of Risk Ident, Europe's leading provider of new intelligent anti-fraud software. Roberto sits on the European Advisory Board of the Merchant Risk Council and is a regular speaker on Europe's anti-fraud conference circuit.

About Risk Ident: Risk Ident is an anti-fraud software development company based in the US and Europe that protects companies within the ecommerce, telecommunication and financial sectors. Our machine-learning software uses sophisticated data analytics to block payment fraud and account takeovers, all with human-friendly alerts that simplify a fraud prevention team's decision-making process.

www.riskident.com

Click here for the company profile

Share this story

RISK IDENT

How is Artificial Intelligence (AI) used to prevent fraud?

Hackers and fraudsters are a constantly moving target; the moment you frame them, they adapt to the surroundings, devising an even more creative and menacing means of attack. For years, fraud prevention was conducted using large sets of rules that would make decisions based on basket value, location of delivery, customer account age, etc. For modern fraudsters, this is far too easy to work around. The 'trial and error' principal means that if they hit a wall, they can just change the parameters and try it again. Large merchants are subsequently hit with thousands of fraudulent transactions from different accounts and different identities every few minutes, 24/7.

Machine learning works on a rule-basis as well, but the difference is that the machine defines these rules and can change them instantly, responding to new threats without human interaction. The technology recognises patterns and regularities in datasets, and is then able to learn from each transaction and a wealth of historical data. In this way, it can continually create new models and constantly evolving algorithms that find patterns, calculate risks and halt illicit activities – in real-time.

However, machine learning doesn't mark the death of human interaction. Experienced fraud managers are still critical in the training process, constantly feeding their knowledge on the context and causes of fraud into the machine, allowing the system to evolve continually. Businesses that combine these human and machine elements can scale their fraud protection system, allowing it to grow, evolve and adapt to changing threats.

Credorax

Securing Ecommerce Payments and Fighting Fraud with AI

As online banking and ecommerce channels are growing exponentially, fraud within these channels becomes more prevalent and damaging. In fact, the total number of ecommerce breaches, according to Experian, has **increased 56%** compared to 2016. Nevertheless, Artificial Intelligence (AI) and machine learning promise to radically shift the balance of power between merchants and the criminals who seek to steal from them.

The growth in digital payments and transactions has left merchants, PSPs and ecommerce companies vulnerable to sophisticated new cyberattacks. Furthermore, the number of people adopting the use of apps and mobile connectivity for making transactions is growing at an astounding rate. This is why, in part, technologies such as Artificial Intelligence (AI) and machine learning are critical in helping organisations fight fraud in better and more effective ways than ever before.

AI is an important development for the payments and transactions industry because merchant business models are evolving daily, from next day delivery of goods to digital downloads. Machine learning used in order to fight fraud is the logical solution for navigating this ever-changing landscape. Other anti-fraud systems using analytics that do not utilise machine learning capabilities, flag credit card purchases that take place outside a customer's country of residence, for example, or unusual payments to remote suppliers. The problem with such systems is that those rules are created by humans, who cumulate and combine data and intuition. It has been proven to be somewhat effective, although the approach can be costly, slow, leading to false positives, and failing to keep pace with emerging trends.

Machine learning detects fraud in real-time and learns from trends, identifying quickly emerging fraud patterns. By integrating and analysing changing, unstructured, and fast-moving data in ways that humans alone cannot do it, machine learning employs the running of multiple self-learning algorithms in parallel to increase fraud detection and prevent it. Additionally, it can identify rare or never-before-experienced fraud events, automate tedious tasks and provide an anti-fraud solution that allows merchants, PSPs and their customers to rest easy knowing they are being protected by a sophisticated approach.

Even though this is an important development in fighting fraud and it is true that machines can better perform the arduous task of evenly sifting through massive sets of structured and unstructured data for fraud patterns, it is still critical to note the role humans play and how company culture must support it.

This is even more so the case since commerce operates in an omnichannel environment across multiple devices and touchpoints. Bad experiences, such as chargebacks, caused by fraudulent activity increase and subsequent losses in online marketplaces, impact those touchpoints that connect buyers and sellers.

Cyber-criminals have familiarised themselves with the ins and outs of payment processes. According to the Nielsen report, fraudsters steal about 5.65 cents per every USD 100 spent. Occurrences of identity theft, phishing and account takeover are ever increasing. It stands to reason why credit cards are the most popular target for fraud. It does not take much to conduct a 'card not present' transaction for online payments. Moreover, the dark web has provided a platform for a relatively easy exchange of stolen data.

These hi-tech hackers have become savvy in detecting vulnerabilities in systems, and pinpoint those backdoors in order to compromise the system and commit fraud. They utilise distributed networks, big data and the dark web to locate these vulnerabilities and optimise their financial gains. In fact, they are devising multidimensional tactics that inflict damage by sequentially compromising more than one point of vulnerability.

Machine learning provides a powerful solution that is responsive and dynamic, user-friendly and easy to maintain. Legacy-based rules of anti-fraud systems are breaking down at this level of sophistication, speed and scale. They lack in performing analytics and delivering risk scores very efficiently. In addition, they are not typically operating in real-time and with the same level of accuracy. ➔

Fiona Brown

SVP of Commercial risk and underwriting
Credorax

About Fiona Brown: Fiona Brown has operated within the field of Risk Management for more than 20 years. She has always worked within Payments and has experience both within Acquiring and PSPs, having held senior roles at both First Data Merchant Services and Pay360 (formerly PayPoint Online). She joined Credorax in April 2017 where she assumed responsibility for the Fraud and Risk teams.

About Credorax: In 2007, Credorax saw an opportunity to change the landscape of traditional merchant acquiring by using its technology assets to address the needs of online merchants of all sizes. This led the company to evolve into a Merchant Acquiring Bank specializing in cross-border ecommerce, with more than 200 employees globally and operations spread across Europe, the US, UK, Malta, and Israel.

www.credorax.com

Share this story

credorax

Machine learning can help by acknowledging behaviour to achieve better and more effective decision-making. This can be applied when conducting identity verification, payment authorisation, checkout scoring and merchant underwriting. The underlining result is that it significantly reduces fraud loss and chargebacks.

Overall, online fraud is expected to continually evolve to keep pace with the rapid development of technology. All the constituents in ecommerce, from merchants and PSPs to financial institutions, must stay ahead of the curve in order to protect themselves. The ramifications of failing to do so can be grim, making it vital to realise and embrace the power of machine learning and AI technologies to detect and prevent fraud in all ecommerce channels.

Europe's biggest FinTech event is coming to Amsterdam

Use the code **18PAYP**
to save **€200** on your pass

4th – 6th June 2018
The Rai, Amsterdam,
The Netherlands

Money EUROPE 20/20

Best Practices in Fighting Fraud

Accertify

Fraud Mitigation – Sharing Makes Us Stronger

You are not alone

Ten years is a long time in the online fraud space. Although the internet has been a way for consumers to transact for much longer than this, it took time for fraud to really make a dent in company profits. As the problem has grown and fraudsters' sophistication has increased, companies have had to balance keeping losses at bay while not impeding growth and future profitability.

It is often the case that the person responsible for fraud is a lone ranger in their company. Internal resources are often tight and training budgets are limited. It can feel incredibly daunting and lonely, especially when facing more frequent and sophisticated fraud attacks. The job can involve a lot of trial and error, but a sound foundation helps to target the focus in the right direction. This can often be sought from peers across the ecommerce world – and yes, sometimes even from competitors.

Learning and understanding what others have experienced can be incredibly powerful, whether on an ad hoc or systematic basis.

We are here for you

At Accertify we signed our first enterprise customer ten years ago and since then, we have focused on three core principles: Community, People and Technology. The sense of Community was initially built on the strong relationships we had with our customers, a function of our second principle: hiring respected industry experts to join our team. Starting in ticketing and quickly growing into travel, retail and financial services, we were able to connect industry peers to enable them to analyse the trends they were seeing and learn ways to mitigate them. This is a powerful forum which we continue to facilitate today on a global basis, organising industry events and discussions, which continue to add value and support industry experts who may otherwise feel they are fighting the battle alone and in the dark.

Our Managed Services team also delivers against this second principle: they are experienced professionals who have expertise across many clients and industries. This means that as they support our clients in the review of transactions, they bring with their assessments a deep understanding of emerging trends across the world and the ecommerce industry. This insight enables them to quickly spot new trends versus a fraud team operating in isolation.

As we have continued to evolve, the community concept has progressed to our third principle: Technology.

Community and technology combine to enable success

We have evolved and expanded our community data to drive better fraud decisions. Our first community data service, Accertify® Risk ID, enables companies to understand more about their customers in real-time, and to benefit from the experience of the Accertify community, even if a customer has never previously shopped with a specific company. ➔

Catherine Tong

General Manager
Accertify

About Catherine Tong: Catherine Tong is General Manager for Accertify in EMEA, leading a team of fraud specialists. With over fifteen years' experience in fraud prevention, before joining Accertify, Catherine held various senior risk roles at retailer Tesco and PwC.

About Accertify: Accertify Inc., a wholly owned subsidiary of American Express, is a leading provider of fraud prevention, chargeback management, and payment gateway solutions to merchants' customers spanning diverse industries worldwide. Accertify's suite of products and services, including machine learning, help ecommerce companies grow their business by driving down the total cost of fraud and protecting their brand.

www.accertify.com

Click here for the company profile

Share this story

Accertify
AN AMERICAN EXPRESS COMPANY

We continued our development with Accertify® Index which uses our machine learning capabilities to assess a combination of data elements across our participating client base in order to provide a positive or negative index of whether the customer is good or bad. Whilst community data services should not be treated as a sole indicator of fraud, both Accertify® Risk ID and Accertify® Index can be powerful tools in a fraud manager's toolbox.

This year, we are taking our machine learning a step further by introducing industry specific community decisioning models, boosting fraud prevention performance. These models can be used in addition to risk rules and will adjust in real-time as they learn from the new transactions fed into them. The power of these shared data points means that companies can benefit from the wisdom of the crowd, understand the community's experience with a customer and help make an informed fraud decision. This community insight provides additional confidence when assessing the risk of a new customer by incorporating millions of data points from the participating Accertify community coupled with the company's proprietary fraud knowledge. Remember – the fraudsters are working together so businesses need to do the same. If we are not pooling resources on our side, then it is inevitable that the bad guys will be able to continue their activities undetected for longer, which increases costs and risk for any business.

ACI Worldwide

Why the Answer is an Analyst

Fraud detection and prevention requires efficient processes, high performing teams and advanced technology. Above all, it needs human intelligence and expert analysis.

With increased consumer choice comes increased opportunity for fraudsters. The growing variety of channels, payment types and fulfilment methods has created a fast changing payments landscape that brings huge challenge for merchants.

Striking the right balance between fraud prevention, conversion and customer service requires a dynamic, multi-faceted risk strategy. For many merchants, one of the most vital components of this strategy is the human one – the expert risk analyst. Having the right people in place to support your strategy plays a critical part at every stage in effective fraud prevention – and experienced analysts go beyond prevention, to create fraud management strategies that enable business growth and new revenue streams.

Knowledge is power

Access to a wealth of data is one of the most critical resources in fighting fraud while enabling genuine consumers enjoy great customer experience– but turning that data into actionable intelligence can be a real challenge. Fine tuning fraud prevention strategies in line with changing trends and customer behaviours requires continuous, proactive analysis of available data. At ACI, we believe this process is most effective when it is driven by dedicated fraud experts – experts who appreciate the fraud challenges unique to a merchant's business and who can select the most appropriate, effective rules and strategies in support of that business's growth targets and Key Performance Indicators (KPIs).

Getting the best from technology

Whether a merchant uses predictive modelling capabilities, a rules-based engine, or both to detect fraud, these solutions need to be tailored, implemented, monitored and adjusted by fraud experts. Technology should be working continuously in the background, updating, flagging and linking fraud and profiling risk. Analysts should be immediately taking this data / intelligence and, with it, fine tuning fraud rules, adapting strategies and constantly enhancing the KPIs that drive bottom line profits.

Fraud rules and predictive models must be built on a thorough understanding of the data available (internal and external) and rules must be adapted in line with seasonal promotions, emerging trends, merchant objectives and market developments.

Expert analysts can also deliver value to other parts of the business. Geographic expansion, product diversification and the introduction of new payment types all carry their own unique set of risks, on which analysts can advise and for which fraud strategies can be adjusted. It is this level of tailored, expert support which can make a good fraud detection system into a highly effective holistic fraud and risk management solution.

Supporting timely action

Fraudsters are becoming increasingly sophisticated as they test for, learn and exploit our weaknesses. They are moving faster and their activities must be shut down more quickly. This is why proactive detection and prevention by expert analysts is so important.

By using business intelligence and analytics tools combined with system alerts, knowledgeable analysts can examine transactions, monitor rules performance, assess patterns and identify emerging trends in real time, spotting and stopping fraudulent activity in its tracks.

This is particularly important during major incidents, when merchants need to know instantly how they have been affected and what action to take to support customers. The ability to rapidly analyse and report on incidents can make all the difference to reputation management, as well as limiting losses.

But risk analysts do not only work on transactions in real time. They will often continue to investigate a transaction long after it has taken place. Further screening – one hour, 24 hours, 72 hours or 30 days after the original transaction occurred – can help to build a more accurate, detailed profile of transactions and associated fraud. ➔

Kieran Mongey

Manager, Solutions Consulting
ACI Worldwide

About Kieran Mongey: Kieran is a qualified accountant who has specialised in payments and fraud management over the last eight years. He currently leads consultancy and solution optimisation strategies for merchant customers within Europe, working as part of ACI's global solutions consulting team.

About ACI Worldwide: ACI, the Universal Payments company, powers electronic payments for more than 5,100 organizations around the world. More than 1,000 of the largest financial institutions and intermediaries as well as thousands of leading merchants globally rely on ACI to execute USD 14 trillion each day in payments.

www.aciworldwide.com

Click here for the company profile

Share this story

ACI UNIVERSAL PAYMENTS

Transactions that are initially accepted and later identified as suspect or confirmed fraud can still be recovered – by halting shipments, cancelling bookings and preventing further orders from being processed. In this way too, merchants can reduce chargebacks, shipping costs and product losses.

Fraud expertise at your fingertips

Often working as an extension to the in-house team, the ACI analyst provides deep fraud expertise and global intelligence, supporting loss prevention, customer service and revenue growth.

Beyond real-time

Working with one of our large retailers, our risk analyst team identified additional savings of over GBP 80,000 across a six-month period simply by taking another look at approved orders before they were shipped. This was done across all delivery methods including those with smaller review windows such as Next Day and Click & Collect. As well as the fraud savings, other benefits and savings derived from this subsequent identification included a reduction in chargeback fees, a reduction in physical goods lost to fraud and savings derived from reviewing linked orders to identify associated fraud.

Preventing fraud while enabling good business

High fraud rates made a major international airline extremely risk adverse, causing the company to implement a strict fraud ruleset that, in turn, was limiting their ability to accept good business. Their newly appointed ACI risk analyst thoroughly reviewed the rules, using internal measures to weight efficiency. The analysis highlighted a potential increase in revenue that could result from some careful tailoring of the fraud rules. Accepting these changes led to a decrease in the Deny rate from 15% (the average over the prior six months) to 5%. Total traffic through the online sales channel also increased by around 20%, delivering a major uplift in revenue for the airline.

To learn how risk analysts at ACI can help your organization reduce fraud and support profitable growth, please contact kieran.mongey@aciworldwide.com.

CyberSource

Play by Your Own Rules: How Machine Learning Helps Tackle Fraudsters

Fraudsters have grown more sophisticated. They're more adept than ever at using technology – even big data and analytics – to conduct fraud. And they use it not only to increase the number of fraudulent orders but also to be cleverer about disguising illicit activity. Fraudsters have also worked out the best moments to attack, and how to capitalise on their opportunities. As a result, it's getting tougher for organisations to determine which transactions to accept and which to reject.

For many companies, the answer lies in machine learning. It's an important tool in helping businesses take on fraudsters, especially because it can analyse vast amounts of data. This provides a sophisticated defence against sophisticated attacks.

The more, the merrier

As transactions flow through global payment networks, the data behind each transaction can help provide vital insights. Machine learning flourishes when it's dealing with high volumes of transaction data. By looking at the information to identify high risk or low risk transactions, machine learning gets better at making accurate predictions and guiding businesses to make the right call – and the more data there is, the more accurate it becomes.

Which is your best option?

In general terms, machine learning offers two very different approaches. Static models use huge amounts of historic transaction data to identify historical fraud patterns and work well when they are brand new. However, fraudsters keep on changing tactics, creating pressure for fraud managers to keep up with fresh patterns.

Self-learning models, on the other hand, thrive on new data. They use it to recognise and adapt to the latest fraud patterns. Even so, they're complex; that can make it difficult for people to track, control or adjust what the machine learns.

Machine learning can help with:

- **Simpler real-time decision-making.** Many fraud mitigation platforms use rules to determine which orders to accept and which to reject. But they're manual and time consuming to set up or change. Machine learning makes rules work. It can also speed up data analysis.
- **Greater accuracy.** Criminals continually create subtler, more non-intuitive patterns. People can find it hard to recognise these – but machine learning doesn't.
- **Faster response to change.** Fraud recognition is a constant game of cat-and-mouse. The right machine learning models can use the latest data and update their approach to reflect new trends.
- **Lower costs.** Major technological advances have cut the costs of machine learning and the computing systems that can run it. Machine learning can also reduce costly false positives as well as the time and cost of manual reviews.

But machine learning:

- Depends on receiving good input data, and plenty of it. Without this, the machine can learn the wrong thing and could make the wrong assessments.
- Is a great tool for automating the pre-determined patterns associated with fraudulent behaviours. However, it needs significant expertise and training to be fully effective, especially since fraud trends evolve rapidly.
- Can often be a black box, especially when it uses self-learning techniques. The machine can learn the wrong thing, and its decision making isn't fully transparent.

The best option for fraud prevention is to combine automated machine learning with a rules-based approach, giving businesses more immediate control over fraud decisions. →

About CyberSource: CyberSource, a wholly owned subsidiary of Visa Inc., is the only integrated payment management platform built on secure Visa infrastructure, with the payment reach and fraud insights of a massive USD 384 bln global processing network. For more information, please visit:
www.cybersource.co.uk.

www.cybersource.com

Click here for the company profile

Share this story

CyberSource®

Bringing together the best

CyberSource's fraud management platform, Decision Manager, combines its own unique version of machine learning with its flexible rules-based engine.

Its machine learning model brings together the flexible data analysis of advanced self-learning and the best bits of the static model. It's always learning from a huge amount of data that's constantly updated. That makes it swift and accurate in responding to unique or emerging trends, with the right approach for each situation.

And added to this is Decision Manager's flexible rules-based engine. Rules act as the first line of defence by applying deterministic decisions to an order; when those can't tell a good transaction from a bad one, machine learning steps in.

The rules-based engine uses 260 anomaly detectors, and 15 region, channel and industry-specific risk models, each tuned to identify fraud in different scenarios. Not only can fraud analysts set and adjust the rules at any time, it's easy to see which rules were applied to make a specific decision.

But core to the success of any fraud management platform is data. It's key for greater accuracy and detection. Decision Manager's machine learning and rules-based capability is fuelled by data that's richer and more plentiful. And it's more relevant because it uses more fraud detectors and actual outcomes of past transactions. Decision Manager is also uniquely enabled by more than 68 billion worldwide transactions, processed annually by Visa and CyberSource, creating the world's largest detection radar.

The result? You can spot and handle even the latest types of fraud more efficiently. This means you can help reduce fraud losses, protect your revenue and operate more efficiently. It can also help keep customers happy and returning, making sure they stay loyal and aren't driven away by refused orders and fraudulent use of accounts.

Ethoca

The Many Faces of Friendly Fraud

In rapidly growing sectors like digital goods, the majority of today's card-not-present (CNP) fraud is so-called 'friendly fraud'. Sometimes called 'false claims', friendly fraud happens when cardholders wrongly request refunds for legitimate purchases. With **86% of card disputes believed to be fraudulent**, and a rate of growth in the double digits (Lexis Nexis Total Cost of Fraud 2012-2015), it's no wonder the FBI views friendly fraud as the third biggest problem in ecommerce.

To protect themselves from this growing threat, merchants and issuers are implementing multi-layered fraud detection and prevention systems. Unfortunately, friendly fraud stems from a spectrum of behaviours that are challenging to detect; these are, after all, legitimate cardholder transactions that don't look like typical 'third-party' fraud. Before merchants and issuers can start to get a handle on this problem, they need to better understand its many faces.

The spectrum of friendly fraud

Approximately 28% of ecommerce revenue is lost annually to friendly fraud (MRC Global Fraud Benchmarking Study 2014). It is usually not detected by typical fraud prevention tools because the consumer was a good one until they decided to dispute the transaction. So, how does one devolve from loyal customer to dishonest fraudster?

The spectrum of friendly fraud behaviour ranges from benign to hostile:

- **BENIGN**: Cardholders might mistakenly dispute charges they made because they forgot about them. Or, they don't recognize the vendors listed on their card statement due to confusing merchant descriptors.
- **BENIGN**: Family members linked to the primary cardholder's account might make purchases that aren't known to the primary cardholder.
- **HOSTILE**: Cardholders may dispute a transaction because they regret the purchase and want their money back. Or, they may want to 'game' the dispute process for personal gain.

What's more, even if merchants and issuers suspect that the cardholder is not being honest, they look at the lifetime value of the relationship and focus on keeping good customers in order to drive future sales. This lack of penalties for cardholders who game the system encourages future abuse.

Friendly fraud and false declines

One of the unintended consequences of so many false claims due to friendly fraud is an increase in future false declines. These happen when a merchant or issuer incorrectly declines a legitimate transaction due to the suspicion of fraud. Referred to by some as 'false positives', false declines create a negative experience for the customers involved and reduce merchant and issuer revenue. Some cardholders completely abandon their purchase after a declined transaction, while others look for another online retailer that will accept their card or switch to an alternative card in their wallet. These false positives represented USD 117 billion in lost transaction-based income in 2015 (Javelin Strategy Webinar, "**Sky Rocketing CNP Fraud Jeopardizes Top of Wallet Status**" July 2016).

What can be done to fight back today?

Winning the war on friendly fraud requires implementing solutions capable of addressing this insidious threat in real-time, while simultaneously reducing – or even eliminating – disputes. It also means changing cardholders' behaviours to reduce the likelihood of them disputing legitimate transactions – regardless of whether their behaviour is benign (e.g., an unrecognized transaction) or hostile (e.g., intentionally gaming the system for personal gain).

Solutions that enable issuers and merchants to present detailed purchase data to cardholders, and help them "recognize" unfamiliar transactions, will increase the number of cardholders who accept liability for their transactions and eliminate the costly chargeback dispute process. This new class of solutions will also address the increasing trend toward abusive, repeat dispute behaviours. The significance of this repeat behaviour was recently illustrated to us by one of our merchant customers who estimates that 40% of cardholders who realize how easy it is to file a false claim will do so again within 60 days. ➔

Keith Briscoe

Chief Marketing Officer
Ethoca

About Keith Briscoe: Keith Briscoe leads Ethoca's global marketing strategy, programmes and day-to-day execution, including the launch of Ethoca's growing range of collaboration-based fraud mitigation and transaction acceptance solutions. His responsibilities include public relations, integrated campaigns, competitive analysis, experiential marketing, product marketing and communications. Keith has more than 15 years of experience in the payments and transaction processing industry.

About Ethoca: Ethoca provides collaboration-based technology solutions that close the information gap between card issuers and ecommerce merchants. Their solutions help global customers stop fraud, eliminate chargebacks, recover lost revenue, and increase card acceptance. They serve more than 580 card issuers and over 5,400 merchants worldwide, including the top ecommerce brands.

www.ethoca.com

Click here for the company profile

Share this story

ethoca™

What does the ultimate solution look like?

Today's best practices focus on effective recovery methods which help to reduce losses attributed to friendly fraud. Unfortunately, they're not a long-term solution and may disrupt the customer experience. For one, a customer who disputes a charge that is ultimately deemed legitimate will need to be rebilled by the issuer – potentially causing that customer more frustration and confusion. It's a vicious cycle that erodes customer experience over time and increases dispute volumes and associated calls for card issuers.

The better solution to winning the war on friendly fraud is reducing or eliminating cardholder disputes proactively and in real-time through new innovations powered by issuer-merchant collaboration. This solution is focused on helping cardholders recognize their own transactions, or those of someone in their household. More importantly, it allows merchants and card issuers to collaborate in a pivotal 'moment of truth' that sets the stage for a superior customer experience.

Self-service tools via the online statement or mobile app would allow the cardholder to have immediate insight into a potentially questionable transaction – without ever needing to contact the merchant or their bank. This would completely remove the element of friction from not only the immediate dispute process, but also future potential purchases (i.e., the painful claims process and card re-issue experience can be avoided entirely, ensuring no disruption to future spending).

A fraud and dispute prevention tool based on real-time collaboration between merchants and issuers would potentially eliminate and greatly reduce the need for chargebacks. Furthermore, it will lead to a more satisfying purchase experience for customers, merchants and issuers alike. Not only would merchants and issuers reduce costly chargebacks, but customers in this new universe would be free from unnecessary purchase disruptions and feel better and more confident about using their cards to shop. Ultimately, both card issuers and merchants would reap the financial rewards that come with a truly frictionless customer experience.

Signifyd

Old Fraud, New Approach: How to Mine the Value of False Positives

The marketing world is awash with buzzwords – those light-as-air, sophisticated-sounding, but often hollow collections of syllables that serve as a glue for the message you would like your audience to embrace, without exactly examining it.

In the business of online fraud protection, the phrase "false positives" is rising to the top of the buzzword heap. It's a real thing, but the term is vague, confusing and often misused. In fact, I prefer the term 'insult rate' to describe the percentage of legitimate orders falsely declined. After all, withholding orders from your legitimate customers is one of the easiest ways to lose a customer.

That said, it's time to give false positives some love.

Ecommerce fraud protection has evolved rapidly, requiring a shift in thinking. The biggest innovation in fraud prevention has been the emergence of Guaranteed Fraud Protection – the notion that liability for chargebacks and fraud costs shifts from merchants to companies that specialise in machine learning-based fraud management.

Disruptive technologies and business models require disruptive thinking. In the case of Guaranteed Fraud Protection, the required reset is the realisation that the goal of fraud protection is not to prevent every incident of fraud.

In fact, in order to achieve true fraud protection, merchants or their fraud vendors must be willing to ship orders that they are convinced are fraudulent. They need to test the bounds of what is fraudulent and what is legitimate. They need to go up to the line representing fraud and then step over it.

Automated fraud systems learn from their mistakes

How else are smart machines going to learn all the permutations of fraud – or all the different looks a legitimate order can display? The sophisticated criminal rings engaged in online fraud are constantly changing tools, targets and tactics. The only way for machines to keep up is to experience the new twists firsthand.

Think of the tactic as the fraud-prevention equivalent to a vaccine to prevent disease. A vaccine contains the very antigen that causes the disease. It's how the body learns what to combat.

In the case of fraud, shipping orders that a machine deems fraudulent is how an enterprise learns what fraud looks like. In fact, if your orders never result in a chargeback, your model is likely holding back too many orders.

As it is, retailers are not doing a very good job of finding the line between fraud and legitimate orders. Business Insider reported that incorrectly declined orders **cost merchants USD 8.6 billion** in 2016.

And the situation isn't getting better. Digital Transactions reported that **35% of the order**s rejected by large retailers turned out to be legitimate – up from 25% in 2016.

Now, purposely shipping apparently fraudulent orders is hardly a sustainable business plan for an individual merchant. First, there is the financial cost to the business. Second, there is the problem of explaining to bosses and investors why you appear to be throwing money away.

This is where Guaranteed Fraud Protection comes in. The promise, which has been recognised by consultants and others as state-of-the-art fraud protection, shifts financial liability away from merchants and onto partner companies that are experts in fraud protection.

The guarantee means that the vendor will financially cover the merchant for any approved order that turns out to be fraudulent. A fraud protection vendor is able to take on that risk because it sees millions of transactions across thousands of merchants. →

Stefan Nandzik

VP of Marketing
Signifyd

About Stefan Nandzik: Stefan Nandzik is the head of marketing at Signifyd. His "what if" approach to business problem-solving constantly challenges conventional wisdom and means that he is never afraid to upend the status quo to lead change

About Signifyd: As the world's largest provider of Guaranteed Fraud Protection, Signifyd delivers a 100% financial guarantee against fraud and chargebacks on every approved order. This shifts fraud liability, allowing you to increase sales and focus on your core business. Signifyd customers include Fortune 1000 and Internet Retailer 500 companies.

www.signifyd.com

Click here for the company profile

Share this story

SIGNIFYD

Shipping fraudulent orders is R&D

It also means that the vendor can afford to – and in fact needs to – allow some orders through that appear to be fraudulent. The cost is akin to investing in research and development. The machine models learn from the fraud and from legitimate orders that were originally believed to be fraudulent. The data the vendor relies on becomes more valuable in the process.

In the end it's all about data. Signifyd, for instance, invests significantly in third-party data from world-leading companies that provide high-quality information on devices, physical and cyber addresses, real estate records and more.

Therefore, leading fraud-management innovators are willing to invest to develop the data yielded by shipping orders initially identified as fraudulent. It is, in fact, data that money can't buy. It's the new paradigm that Guaranteed Fraud Protection enables.

Think about it: Everybody in ecommerce talks about making better fraud decisions and about reducing or eliminating false positives. But how? How do you do that, exactly?

Fraud feedback must include unexpected outcomes

Fraud protection systems that don't understand the value of allowing apparently fraudulent orders to ship are stuck pushing their learning machines in a conservative direction. If every bit of feedback a machine ingests is the result of a chargeback due to fraud, that machine is going to ratchet back with every new data point.

If you also feed the machine some surprising results – feedback from orders that shouldn't have been allowed through, according to current models, but that were in fact legitimate – then you're achieving true learning. Your revised model will know to allow more orders to ship.

Think of it as the investment you need to make in order to discover the positive in false positives.

PwC

PricewaterhouseCoopers

As building trust is part of a financial institution's development, security and privacy should be inherent to this process. PwC offers valuable insights on how to avoid cyberattacks and become a reliable financial services provider.

Which were the biggest cyber threats that 2017 has brought to the online banking sector?

The cyber threats have been increasing generally over the last few years, as our digital dependency continues to rise. One of the most common ways into an organisation is still to target customers or staff directly via emails or phone calls to gain access to systems or to trick an individual into transferring payments to another bank account. We've also seen a sharp rise in ransomware attacks, which prevent access to systems unless an unlock fee is paid, plus automated attacks aimed purely at causing the maximum damage to systems.

Because of the potential rewards on offer in the banking sector, cybercriminals are investing time to understand the intricacies of how business processes and systems work, as seen with recent attacks on payment networks. Hackers have found ways to access these networks by exploiting the vulnerabilities in several banks' systems. This has enabled them to create untraceable malware, allowing them to transfer large sums of money around the world.

> *"With attackers getting ever smarter, banks need to shift their thinking from protecting the perimeter to embedding cyber resilience.*

Under the current security context, what are your recommendations for banks? What should they be aware of and how can they prevent fraud more efficiently?

With attackers getting ever smarter, financial services organisations need to shift their thinking from protecting the perimeter to embedding cyber resilience into their organisation – looking at how business processes work and where the potential weaknesses might be.

It's important to think about your risk profile and know your data: what you have, where it is, what it is used for, and what third parties you rely on to protect it. Once you know the facts, then you can build an effective targeted strategy to secure your critical assets.

Make sure you're investing in the right areas and don't wait until it's too late. So many of the large-scale attacks happen by exploiting simple known vulnerabilities. You need to have the right skills in place to monitor systems for suspicious behaviour or access, but also to back up data and patch systems regularly. Educating staff, building awareness amongst customers and working with secure partners is also key.

Cyberattacks are now a case of 'when' rather than 'if', but our recent **Global State of Information Security Survey** found that nearly one in five UK organisations admit they don't prepare for when the worst does happen. Having an incident response plan in place, and testing it regularly, is essential to make sure that everyone involved knows what to do in a crisis.

What opportunities will General Data Protection Regulation bring for bank customers and what regulatory challenges will it bring for financial institutions in terms of data privacy?

One of the primary aims of the GDPR is to give more control to the consumer over their personal data, including increased rights around the collection and processing of personal data, and more visibility into how it is used. The right to data portability also means that customers will be able to move from one bank to another more easily, with direct transfer of personal data. ➔

Ian Benson

Partner
PwC

About Ian Benson: Ian is a Partner in PwC's Financial Services practice. He has over 17 years' experience working with banks and other financial institutions to help them understand and manage their cyber risk.

About PwC: At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 157 countries with more than 223,000 people who are committed to delivering quality in assurance, advisory and tax services.

www.pwc.co.uk

Share this story

Apart from the obvious regulatory challenges that the GDPR introduces, such as fines of up to 4% of global turnover, we are seeing many financial institutions trying to tackle the operational challenges involved, so they can effectively and efficiently:

- Know where personal data is being stored and transferred to, so they can have the right controls in place;
- Appropriately manage and change the data in line with customer requests and expectations;
- Identify and respond to data breaches immediately, including notifying regulators and data subjects promptly.

Whilst this is not an easy challenge, the most forward-thinking organisations are those that approach this not purely as a compliance exercise, but consider how they can use this opportunity to rethink operations. Getting your data privacy approach right can be a business differentiator, while also bringing a competitive advantage.

What actions has PwC been taking for 2017 in order to help financial institutions prevent fraud? Can you share some plans and predictions for 2018 as well?

This year, we have been working to establish several joint business relationships with innovative technology companies to improve fraud detection with advanced analytics. When it comes to investigation work in large-scale fraud cases for our clients, this helps understand root causes and then strengthen the controls in place.

In 2018, the trend of open banking (and associated regulations like PSD2) will introduce new potential channels for fraud within the payments and banking ecosystem. These need to be handled with the right combination of business, risk and technology considerations.

We'll see a stronger focus on digital identities and multi-device customer authentication. But also the continued increase in popularity of machine learning and behavioural analytics tools, with many advanced systems being deployed across the industry.

AI Detection

The Evolving Risk of a Career in Risk

Having initially been a manual reviewer, then a team leader and a manager, I always kept my focus on offering support to my employees – treat them with respect and help them grow professionally. However, I sadly witnessed good employees change their career path, solely because they didn´t have a chance to grow at their own pace.

Recently, I have been witnessing an increased demand for risk analysts, manual reviewers and managers. In the past years, the main source of manual review agents was Customer and IT support, but good leaders opened their doors to other types of degrees, such as mathematics and statistics, creating a first wave of smart analysts. Now the market request shifted to Risk Analysts and Managers, and it seems that the role of manual reviewer is not the most looked for anymore.

From one point of view, companies' requests shifted to more senior positions. Analysts with few years of experience, team leaders, managers, supervisors and so on, aim for jobs of higher management in companies who had to implement or improve a risk solution for their ecommerce traffic.

And exactly this evolution is what we can find on the market. Many players from the payments ecosystem decided to look at risk solutions. Numerous merchants did the same, either by building an internal solution or by outsourcing part of the business to external experts.

Some companies gave their best employees the opportunity to promote to higher positions with a new perspective on how to detect fraud and what to do with it.

Others decided to outsource to providers with more expertise, cutting internal costs (and heads).

Let us remember that we live in a very fast-paced environment. This article is pertinent to the date of publication. In only a few months, companies where good employees have been promoted and rewarded will be making not only better savings (usually by implementing new solutions based on Machine Learning), but will also be able to process more orders with a highly improved revenue for merchants.

Of course, there are plenty of different outsourcing providers out there, some extremely good and efficient. Your boss may request a business plan on the hypothesis of firing you. But the company might have the opportunity of becoming more profitable. And there are also other providers that will simply claim they have the expertise and kill your store sales instead.

A stronger internal platform is still the best solution, if you have the budget for it. Otherwise, do your research and find the right one that suits your needs.

A good recent example came from a presentation done by a travel industry provider – incredible results were achieved while reducing costs, fraud losses and increasing acceptance rate, all by implementing internally a Machine Learning system to prevent and detect fraud. Employees from the manual review department have been promoted to other positions and other types of risk prevention.

Of course, each career has its own development path(s), but until now, Manual Review agents were the last ring of a chain with limited exit points. Clearly, there are positions, such as supervisors and team leaders, but going further up means that new vacancies appear along the way. When the business and volumes stay the same, employees will get burned. I referred to this in my writings as an "expiration date" and things haven't changed that much. →

Edoardo Fiorentini

CEO and co-founder
AI-Detection

About Edoardo Fiorentini: Edoardo "Edo" Fiorentini is the CEO and co-founder of AI-Detection, an innovative recently launched ecommerce risk management solution, based on Artificial Intelligence paired with Machine Learning and other technologies. Author of **"How to get away with e-commerce fraud"**, Edo has been a presenter and trainer for different risk organisations of the industry.

About AI Detection: AI Detection was founded in Barcelona in the summer of 2017, on the concept of providing an AI management of Machine Learning modules for risk prevention. Using the most advanced theories studied in universities in USA and Israel to improve self-managed models for risk scoring, we are currently working with several merchants to help them improve their ability to accept more customers.

www.aidetection.com
www.edoreloaded.com

Share this story

AI DETECTION

Except for some businesses. Rather than hiring an expert analyst who doesn´t know your business, it makes more sense to promote an experienced manual review agent, if he can learn the additional skills and understanding. Clearly, you can´t promote your whole team. Someone doesn't deserve it, others may not be suitable, the rest… must fight for one single position.

While these workers are busy with preventing fraud on your platform (and accepting false positives), you are also going to put in their minds the fight for career advancement. Instead, you should already know who are your most brilliant and promotion suitable employees. Groom them, let them improve their world first. The rest will naturally follow.

Just remember, you are not looking for a leader, but for experienced professionals who can improve your business. And someone who already knows your risk metrics is not going to ruin the system; instead he/she will improve it – with lots of enthusiasm.

In the last few years, I've seen multiple friends getting to the next level, but the clear majority did it by jumping ship from one company to another. Now this is changing. HR may have understood, at last, that human resources mean employees. Mind blowing? I think not.

Smart businesses are leveraging internal professionals and creating opportunities, focusing on allowing employees to learn new skills for real career advancement. Dumb businesses are letting their employees fly elsewhere because they are not really evolving and reaching the next step. Sure, outsource everything and have fun. Pray that the owner of the company won't decide to outsource your position, as well.

DUBLIN

RISK IDENT
Overall Sponsor

MRC DUBLIN 2018

14-16 MAY, 2018 | The CCD Dublin, Ireland

REGISTRATION NOW OPEN

Early Bird Savings!

All Attendees Save €200+ With Early Bird Discounts

600 attendees

70+ speakers

65+ sessions

45 exhibitors

Delivering 3 Days of Top Tier Content

Beginner, intermediate, advanced tracks

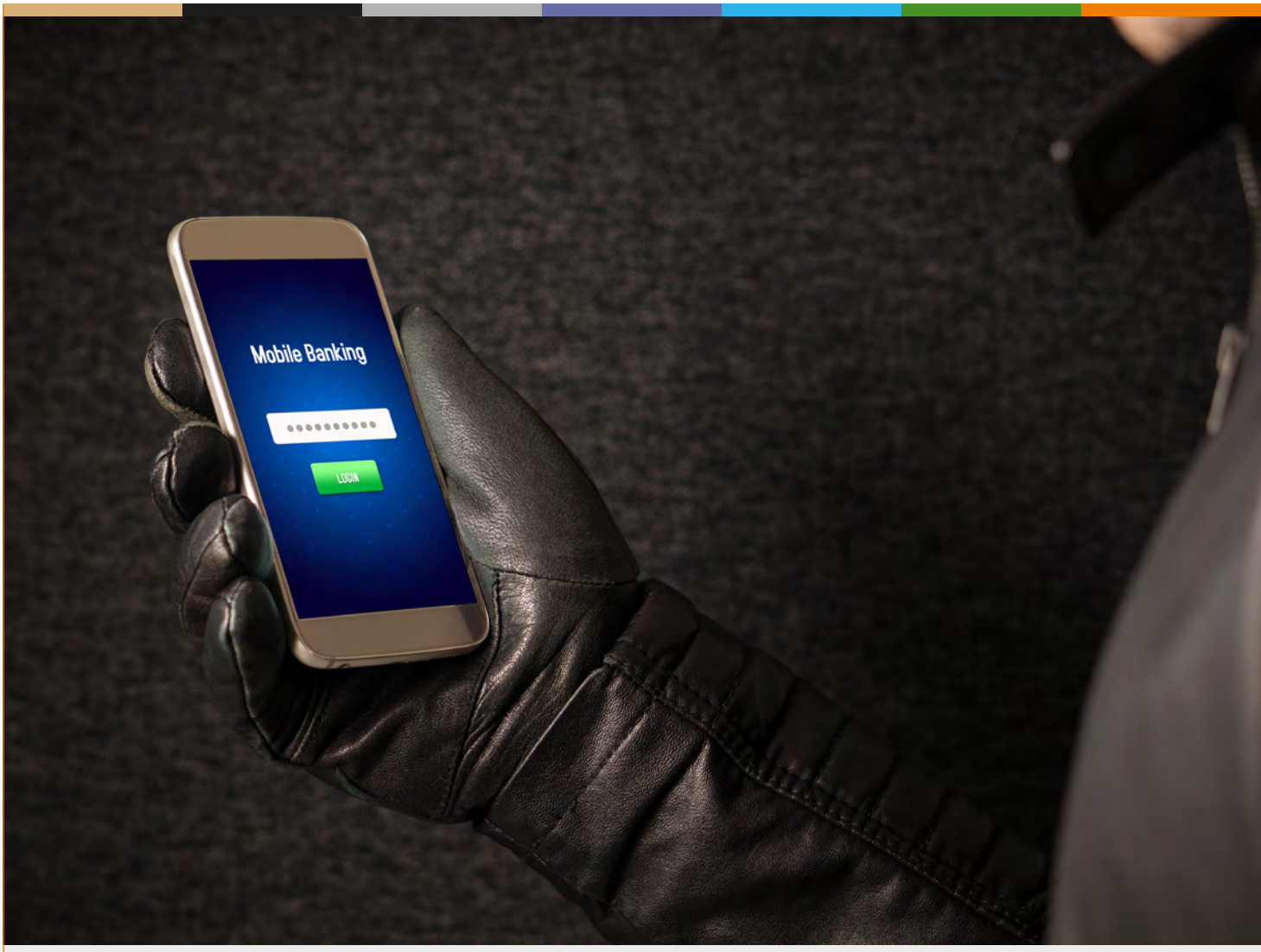
Global Payments Survey results, partnered with CyberSource

Opening Reception at Guinness Storehouse, sponsored by Verifi

Women in Payments and Fraud, sponsored by J.P. Morgan

Dozens of networking events

Find out more here: https://events.merchantriskcouncil.org/mrcdublin18/



Regulations and Directives – Opportunities, Obligations, and Obstacles

Merchant Risk Council

Fraud Reporting Requirements under PSD2

The European Banking Authority (EBA) has released two sets of draft guidelines on fraud reporting requirements under Article 96(6) of the revised Payment Services Directive (PSD2) that will take effect on the 13th of January 2018.

What are these guidelines?

These guidelines should assist in regulating the challenges facing the financial industry as cyberattacks and loss of data become more prevalent. The legal ramifications and economic effects have significant impacts on the reputation and infrastructure of banks and financial institutions.

Regulations become increasingly important in supporting the PSPs' efforts for detecting and classifying operational and security incidents, while implementing management procedures. Because of this, a closer look into notifiable incidents was necessary. Both sets of guidelines are distinctly different.

These guidelines list the criteria needed to assess if an operational or security incident is of sufficient magnitude to warrant external notification. These include the total value and number of transactions and payment users affected, downtimes, economic and reputation impacts, and whether additional infrastructures or other payment services were affected. The EBA has decided not to treat distinctly the issues experienced by different types of PSP.

The first set includes the following:

- Requirements that apply to all PSPs, except for account information service providers;
- The definition of "fraudulent payment transactions" as it relates to data reporting;
- The methodology for collating and reporting data, which includes reporting periods, data breakdown, reporting deadlines and frequency.

The PSPs are all expected to disseminate high-level data on a quarterly basis, with more comprehensive information annually.

The second set of guidelines outline the requirements for the regulatory authorities on data aggregation, data reporting frequency and deadlines that apply to the ECB and EBA.

Why were these guidelines developed?

Data on payment fraud in the EU has been difficult to obtain, not reliable, and has inconsistencies among the Member States. According to Article 96(6) of PSD2, payment service providers (PSPs) must provide "statistical data on fraud relating to different means of payment to their competent authorities." The overall goal is to obtain reliable, comparable data for all EU countries as it relates to payment fraud.

Who do these guidelines affect?

These guidelines address specific PSPs and other banks, and aim to regulate the reporting requirements for payment fraud. Small PSPs only face an annual reporting duty.

What should be reported?

There are three types of fraud cases that should be reported:

- Unauthorised payment transactions, including those resulting from the loss, theft, or misappropriation of a payment instrument or other sensitive payment data, regardless of detectability or root cause;
- Payment transactions made and authorised by a payer that acted dishonestly or by misrepresentation, regardless of intent;
- Payment transactions made as a result of the payer being manipulated.

There are certain rules that accompany these cases. Only fraud payments that have been initiated and successfully executed need to be accounted for in the PSP disclosures. Any cases of attempted fraud that have failed do not require reporting. ➔

Markus Bergthaler

Director of Programs
Merchant Risk Council

About Markus Bergthaler: Markus oversees the development of all Association programme content, conference education, committee and community subject matter, website content, benchmarking, and online forum topics. Markus joined the MRC from Wizards of the Coast where he led the company's fraud department.

About Merchant Risk Council: The Merchant Risk Council is the leading global trade association for fraud and payments professionals. The MRC provides support and education to members with proprietary benchmarking reports, whitepapers, presentations and webinars. The MRC hosts four annual conferences in the US and Europe, as well as regional networking meetings for professionals to connect, exchange best practices and share emerging trends. #ProudlyACommunity

www.merchantriskcouncil.org

Share this story

Building Better Commerce
Fraud & Payments Professionals

Additionally, both net fraud and gross amounts must be reported under both plans. Gross figures relate to the value of funds defrauded, and net fraud relates to cases where some of the losses have been recovered by the PSPs, including insurance fraud.

Are there any exemptions to these guidelines?

Account information service providers are exempt from reporting requirements to avoid any double counting of fraud cases. It is assumed that PSPs will record these instances.

How should the data be broken down?

The data should be reported separately for each payment service or instrument operated by the PSPs. These include money remittance, e-money, payment initiation services, direct debit services, payment cards issuance, payment cards acquisition and credit transfers.

There are certain categories that should be followed:

- The method of authentication used;
- The reason why the authentication method was chosen;
- The type of fraud.

Data must include the volume and value of fraud related transactions recorded per country within the European Economic Area (EEA), and an aggregate form for non-EEA transactions where at least one part of the transaction is performed in the EEA.

An additional component of the guidelines are templates for the reports that must be submitted by the PSPs during reportable incidents. When an incident originates within a company, it may employ consolidated reporting with other businesses who have affected payments through a service provider. With these guidelines, the EBA has clarified that "near misses" do not have to be reported.

These guidelines should help achieve an accurate snapshot of payment fraud occurring in the EU, including the size, components and development over time. They should also help increase the security of retail payments in the EU.

time.lex

Data Breach Notifications: What's New?

On October 3rd 2017, the EU's Article 29 Working Party (WP29) adopted its draft Guidelines on Personal data breach notification under Regulation 2016/679 [General Data Protection Regulation (GDPR)]. Since the document is still open for comment by stakeholders until November 28th 2017, this article marks the Guidelines' main takeaways and innovations.

What are the main data breach obligations under the GDPR?

Article 33 (1) of the GDPR requires data controllers to notify personal data breaches to the competent supervisory authority, without undue delay and within 72 hours after having become aware of the personal data breach. But when can a controller be considered 'aware'? According to the WP29, the controller will not be regarded as 'aware' until after the short period in which he investigates if a breach has occurred, provided however that this initial investigation begins as soon as possible.

Article 34 (1,3) of the GDPR further states that when a personal data breach is likely to present a high risk to the rights and freedoms of individuals, those data subjects should also be informed about the breach without undue delay (art. 34 (1,3) GDPR). 'Without undue delay' in this case means 'as soon as possible', the WP29 says.

In addition, the GDPR requires data processors who become aware of a personal data breach to notify the controller on behalf of whom they are processing the data. This notification should, according to WP29, take place immediately. Data controllers do well by taking this time limit into account when contracting with data processors, given the WP29's opinion that once a processor is aware, the controller should be considered aware as well (and thus, the 72-hour countdown will start).

When is notification (not) needed?

Not all data breaches should be notified, but only those that are likely to result in a risk or high risk to the rights and freedoms of individuals. For this reason, the WP29 has proposed in its Guidelines several relevant criteria for data controllers to precisely assess the risks that could result from an incident.

However, the WP29 stresses that in case of doubt, the controller should err on the side of caution and notify the possible breach.

Which information should be provided?

When notifying a breach to the supervisory authority, a minimum of information concerning the breach, set out in article 33(3) of the GDPR, should be handed over. This encompasses, among other information, a description of the nature of the breach, including, where possible, the categories and approximate numbers of data subjects and personal data records concerned. While the GDPR does not further define these categories, the WP29 in its Guidelines gives guidance on what types of data subject and data records should be distinguished.

The GDPR recognizes, however, that controllers might not always possess all the information concerning the breach within 72 hours of becoming aware of it, and thus allows for a phased notification. A delayed notification, by means of a 'bundled' notification, is also permissible according to the WP29, but only when upon investigation of the breach the controller notices other similar breaches.

When communicating a breach to affected individuals, article 34(2) of the GDPR also describes the minimum of information that should be disclosed.

And to whom?

Notifications of personal data breaches that are likely to result in a risk to the rights and freedoms of natural persons should be addressed to the competent supervisory authority. The affected individuals should be informed too. In this context, the WP29 indicates that breaches should be communicated to the victims in a clear and transparent way, through dedicated messages (e.g. direct messaging, prominent website banners, postal communications etc.). A mere press release or corporate blog will not suffice. ➔

Edwin Jacobs

Fintech lawyer
time.lex

About Edwin Jacobs: Edwin Jacobs is a partner at time.lex and lecturer at the University of Antwerp. Specialties: business law in the information society, negotiation and legal management of ICT-projects, outsourcing, intellectual property rights, copyright, trademarks, privacy/data protection, e-business, electronic contracting, dispute resolution in IT and IP conflicts.

About time.lex: time.lex is a law firm specialised in fintech, information and technology law in the broadest sense, including privacy protection, data and information management, e-business, intellectual property, online media and telecommunications.

www.timelex.eu

Share this story

Record keeping

Regarding the obligation of record keeping under the GDPR, the WP29 encourages controllers to establish an internal register of breaches, even if the notification is not required. In fact, it recommends data controllers to keep a record of all reasoning and justifications for decisions taken in response to a breach. After all, failure to properly document a breach allows the supervisory authority to exercise its powers and impose a fine, the WP29 notes.

Sanctions

If controllers fail to comply with data breach notifications, even though all requirements are fulfilled, an administrative fine can be imposed as well as other corrective measures. This fine can amount up to EUR 10,000,000 or 2% of the total worldwide annual turnover of an 'undertaking' (that is a parent company as well as all involved subsidiaries). On top of that, a sanction for absence or inadequacy of security measures could be issued, thus putting up to 4% of an undertaking's worldwide annual turnover at stake.

Conclusion

The draft Guidelines on Personal data breach notification under the General Data Protection Regulation that are recently adopted by the Article 29 Working Party provide some much-needed and very welcomed guidance to the breach notification requirements. Companies that wish to maintain a solid data protection management would do well by implementing the Guidelines in their data protection policies. However, merely complying with the GDPR and the Guidelines won't be sufficient, given the variety of other legal instruments that put weighty data breach obligations on the service providers operating in the fields of payments, communications and Internet.

Make sure you check a more detailed discussion on this topic on The Paypers' **website**.

Infographic – Global Mapping of Key Players in the Fraud Management Industry

Infographic of Fraud Management Solution Providers

Fraud Management + Identity Verification + Online Authentication

feedzai
CyberSource
PHONIC
IdentityMind GLOBAL
Digital Identities You Can Trust
EverCompliant
More Intelligence. Less Risk.
ThreatMetrix
Kount
iSignthis
FEATURE SPACE
RSA
Perseuss
simility
worldline
e-payment services

Fraud Management

ACI payment systems
sift science
Move at the speed of trust
Ravelin
features analytics

Guaranteed Fraud Protection

SIGNIFYD
riskified
Fraugster
FORTER
appruvd

Fraud Management + Identity Verification

emailage
The Global Hub of Email Intelligence
WEBSHIELD

Fraud Management + Online Authentication

Accertify
an American Express company
buguroo
emailage
The Global Hub of Email Intelligence
EASYSOLUTIONS TOTALFRAUDPROTECTION
iovation
SECUREDTOUCH
RISK IDENT
BIOCATCH
Less Friction. Less Fraud

Specialized Chargeback Handling

THE CHARGEBACK COMPANY
ethoca
GLOBAL RISK TECHNOLOGIES
eConsumer services

Fraud Management, Online Authentication and Identity Verification

Company	Accertify	ACI Universal Payments	BioCatch	buguroo	CyberSource
Fraud Management					
Fraud Detection					
Target group					
Issuers			x		
Merchants	x	x			x
Acquirers	x				
Technology					
In-House					
Cloud-based		x	x		x
Hybrid	x			x	
Methodology					
Rule-Based	x	x	x		
Machine Learning	x	x	x		
Hybrid	x	x	x	x	x
Intelligence					
Abuse List	x	x		x	x
Monitoring	x	x		x	x
Adress Verification	x	x			x
Credit Bureau	x				
Information Sharing Network	x	x	x		
Case management	x	x			x
Recovery		x			
Guaranteed fraud prevention		x	x		

Fraud Management, Online Authentication and Identity Verification

Company	Accertify	ACI Universal Payments	BioCatch	buguroo	CyberSource
Digital Identitity Verification					
ID verification					
Identity Document Scanning					
Video scanning					
Personally identifiable information (PII) Validation					x
Derived verification					
Small Transaction verification					
Email verification		x			x
Additional checks/compliances					
Credit check					
Compliance check		x			x
Online Authentication					
Behavioral biometrics					
Session analysis	x		x	x	
Device-user interaction	x	x	x	x	x
Physical biometrics					
2-D facial recognition					
Fingerprint scan					
Iris scan					
Other					
Device fingerprinting	x	x	x	x	x
Remote access detection	x	x	x	x	x
Mobile app push	x	x		x	
3-D secure 2.0		x			x
Hardware token					
One-time passwords					
Knowledge-Based Authentication				x	

Fraud Management, Online Authentication and Identity Verification

Company	EASYSOLUTIONS TOTAL FRAUD PROTECTION	emailage	Entersekt	ethoca	FEATURE SPACE
Fraud Management					
Fraud Detection					
Target group					
Issuers		x		x	x
Merchants		x		x	x
Acquirers		x			x
Technology					
In-House	x	x			x
Cloud-based	x	x		x	x
Hybrid	x	x		x	x
Methodology					
Rule-Based	x	x			x
Machine Learning	x	x			x
Hybrid	x	x			x
Intelligence					
Abuse List	x	x			x
Monitoring	x				x
Adress Verification		x			x
Credit Bureau					x
Information Sharing Network		x		x	x
Case management	x				x
Recovery				x	x
Guaranteed fraud prevention	x				x

Fraud Management, Online Authentication and Identity Verification

Company	EASYSOLUTIONS TOTALFRAUDPROTECTION	emailage	Entersekt	ethoca	FEATURE SPACE
Digital Identitity Verification					
ID verification					
Identity Document Scanning					x
Video scanning					x
Personally identifiable information (PII) Validation					x
Derived verification					x
Small Transaction verification					x
Email verification		x			x
Additional checks/compliances					
Credit check					x
Compliance check					x
Online Authentication					
Behavioral biometrics					
Session analysis	x				x
Device-user interaction	x				x
Physical biometrics					
2-D facial recognition	x		x		x
Fingerprint scan	x		x		x
Iris scan	x		x		x
Other					
Device fingerprinting	x		x		x
Remote access detection	x		x		x
Mobile app push	x		x		x
3-D secure 2.0	x		x		x
Hardware token	x				
One-time passwords	x		x		x
Knowledge-Based Authentication	x				x

Fraud Management, Online Authentication and Identity Verification

Company	feedzai	IdentityMind GLOBAL	iovation	Kount	RISK IDENT
Fraud Management					
Fraud Detection					
Target group					
Issuers	x		x	x	x
Merchants	x	x	x	x	x
Acquirers	x		x	x	x
Technology					
In-House	x				x
Cloud-based	x	x	x	x	x
Hybrid	x				x
Methodology					
Rule-Based	x	x	x	x	x
Machine Learning	x	x	x	x	x
Hybrid	x		x	x	x
Intelligence					
Abuse List	x	x	x	x	x
Monitoring	x	x	x	x	x
Adress Verification	x	x		x	x
Credit Bureau	x				x
Information Sharing Network		x	x	x	x
Case management	x	x		x	
Recovery				x	
Guaranteed fraud prevention					

Fraud Management, Online Authentication and Identity Verification

Company	feedzai	IdentityMind GLOBAL	iovation	Kount	RISK IDENT
Digital Identitity Verification					
ID verification					
Identity Document Scanning		x			
Video scanning					
Personally identifiable information (PII) Validation		x		x	
Derived verification					
Small Transaction verification		x		x	
Email verification		x		x	
Additional checks/compliances					
Credit check	x				
Compliance check	x	x			
Online Authentication					
Behavioral biometrics					
Session analysis		x		x	
Device-user interaction		x	x	x	
Physical biometrics					
2-D facial recognition			x		
Fingerprint scan		x	x		
Iris scan					
Other					
Device fingerprinting	x	x	x	x	x
Remote access detection				x	
Mobile app push			x	x	
3-D secure 2.0					
Hardware token			x		
One-time passwords			x	x	
Knowledge-Based Authentication		x			

Fraud Management, Online Authentication and Identity Verification

Company	SECURED TOUCH	sift science Move at the speed of trust	SIGNIFYD	simility	ThreatMetrix
Fraud Management					
Fraud Detection					
Target group					
Issuers	x	x		x	x
Merchants	x	x	x	x	x
Acquirers	x	x		x	x
Technology					
In-House	x			x	
Cloud-based	x	x	x	x	x
Hybrid	x			x	
Methodology					
Rule-Based	x				
Machine Learning	x	x	x		
Hybrid	x			x	
Intelligence					
Abuse List			x	x	x
Monitoring			x	x	x
Adress Verification			x		x
Credit Bureau					
Information Sharing Network			x	x	x
Case management		x	x	x	x
Recovery					
Guaranteed fraud prevention			x		

Fraud Management, Online Authentication and Identity Verification

Company	SECURED TOUCH	sift science Move at the speed of trust	SIGNIFYD	simility	ThreatMetrix
Digital Identitity Verification					
ID verification					
Identity Document Scanning				x	
Video scanning					
Personally identifiable information (PII) Validation				x	
Derived verification				x	x
Small Transaction verification				x	
Email verification				x	x
Additional checks/compliances					
Credit check				x	
Compliance check				x	
Online Authentication					
Behavioral biometrics					
Session analysis	x	x	x	x	x
Device-user interaction	x	x	x	x	x
Physical biometrics					
2-D facial recognition					x
Fingerprint scan					x
Iris scan					x
Other					
Device fingerprinting	x	x	x	x	x
Remote access detection	x	x	x	x	x
Mobile app push		x			x
3-D secure 2.0				x	x
Hardware token					
One-time passwords					x
Knowledge-Based Authentication				x	

Fraud Management, Online Authentication and Identity Verification

Company	WEB SHIELD	worldline
Fraud Management		
Fraud Detection		
Target group		
Issuers		x
Merchants		x
Acquirers	x	x
Technology		
In-House		x
Cloud-based	x	x
Hybrid		x
Methodology		
Rule-Based	x	x
Machine Learning		x
Hybrid		x
Intelligence		
Abuse List	x	
Monitoring	x	x
Adress Verification	x	
Credit Bureau	x	
Information Sharing Network	x	
Case management	x	x
Recovery		x
Guaranteed fraud prevention		

Fraud Management, Online Authentication and Identity Verification

Company	WEB SHIELD	worldline
Digital Identitity Verification		
ID verification		
Identity Document Scanning	x	x
Video scanning		x
Personally identifiable information (PII) Validation	x	x
Derived verification		
Small Transaction verification		x
Email verification		x
Additional checks/compliances		
Credit check	x	x
Compliance check	x	x
Online Authentication		
Behavioral biometrics		
Session analysis		x
Device-user interaction		x
Physical biometrics		
2-D facial recognition		x
Fingerprint scan		x
Iris scan		
Other		
Device fingerprinting		x
Remote access detection		x
Mobile app push		x
3-D secure 2.0		x
Hardware token		
One-time passwords		x
Knowledge-Based Authentication		x

13-15 MARCH 2018

Money ASIA 20/20

The world's largest payments and financial services innovation event is launching in Asia

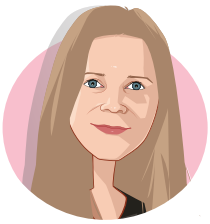
Money20/20 is where the smartest Asian innovators and leaders in payments, FinTech and financial services come together to connect and create the future of money.

Join us at the prestigious Marina Bay Sands in Singapore on March 13-15th 2018 to experience original insight, trailblazing enterprise and high-impact networking.

Agenda themes include:

- **Bits & Blocks: Coins & Ledgers**
- **Data, AI & Algorithm-Based Innovation**
- **Financial Inclusion**
- **Mobile Payments & Wallets**
- **Processing, Instant Payments & Open Platform**

Payment Innovators Include:



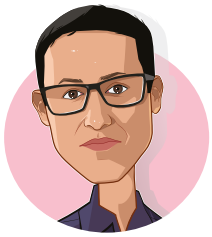
Karla Allen,
Senior Director Mobile Payments
Walmart

Greg Gibb,
Co-Chairman & CEO
陆金所 Lufax

Jonathan Larsen,
CIO
中国平安 PING AN

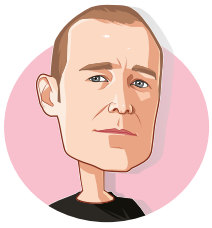
Cheng Li,
CTO
蚂蚁金服 ANT FINANCIAL

Lucy Liu,
COO & Co-Founder
AIRWALLEX



Nadiem Makarim,
CEO & Founder
GO JEK

Ning Tang,
Chairman & CEO
宜信 CreditEase



Pieter van der Does,
Co-Founder/President & CEO
adyen

BOOK NOW WITH AN EXCLUSIVE $250 OFF. USE CODE: **18PP**

Register Online: asia.money2020.com

Customer Identity & Access Management

The ubiquity of mobile devices and tremendous growth in connectivity is fundamental changing the way that individuals bank and access other financial services. A robust digital identity platform is the linchpin to verifying and authenticating users not only to establish trust in online transactions, but also to secure customer trust.

Customer Identity Access Management space presentation

Identity & Access Management, Identity as a Service or Customer Identity & Access Management?

By Rob van der Staaij

Many organizations have implemented an on-premise environment for identity & access management (IAM) to manage the identities of their own employees and their access rights. They are now looking for ways to support new business models and to reduce costs and complexity. This comes with a number of challenges, one of which is that the IAM market is rapidly evolving.

Although the implementation of IAM in the enterprise has more than often taken a number of years for most organizations, these traditional IAM environments are very straightforward. They are restricted to the enterprise itself and the scope mostly encompasses internal users (be it employees, contractors or consultants). The systems and applications that are part of the IAM environment have been predominantly enterprise-based.

These IAM environments are used to support processes like hiring, job or department change and job termination. Usually, the hiring process goes like this: the new employee is registered in the HR application, identity information is provisioned to the IAM environment and a workflow process is triggered whereby the manager of the new employee is notified and asked to assign one or more roles to the employee. As a result, the new employee will be able to perform his or her tasks based on the role(s) and the user account information and authorizations assigned to him or her in the systems and applications. This whole process is called 'user provisioning' or – more generally – 'identity governance'.

Gradually, the traditional IAM environment has been extended to also store information about business partners, suppliers and customers (in this article the terms consumers and customers are used without distinction, since both terms can be used interchangeably in most cases). As a consequence, complex identity federations have arisen, and they include multiple source systems, identity providers, service providers, on-premise applications and cloud applications. In terms of scalability and performance, this is not a problem for modern IAM systems. The product suites of the well-known IAM vendors are without exception very well able to scale into hundreds of thousands or even millions of users.

However, due to these developments, on-premise IAM has become too costly and too comprehensive to manage for most organizations. Moreover, IAM services in general have become more and more complex. The capabilities of modern IAM should not only support traditional (web) applications, but also mobile applications, hybrid mobile applications, APIs (application programming interfaces) and Internet-connected things (also called Internet of things or IoTs). In addition, today's IAM features need to be very extensive and should include identity synchronization, social identity integration (bring your own identity or BYOI), self-service registration, account linking, single sign-on, password self-reset, session management, adaptive and contextual access control, mobile authentication (e.g. leveraging the biometrics capabilities of smartphones), identity intelligence, identity analytics and authorization management. Features that become very relevant to GDPR (General Data Protection Directive) include consent management, the ability for consumers to determine what personal information they are allowing to be used, and the encryption of identity and profile information. →

Identity & Access Management, Identity as a Service or Customer Identity & Access Management?

Those are the reasons why Identity as a Service (IDaaS) has started to expand. IDaaS can be defined as identity & access management that is hosted and managed by a third-party service provider. IDaaS is growing exponentially. Increasingly, more organizations are shifting their identity & access management environment to the cloud and for good reasons. The benefits are comparable to other cloud services: reduced costs, business on demand, reduced need for an on-site infrastructure, and easier management. An additional benefit of IDaaS is the rich feature set that many providers increasingly offer. IDaaS players include the traditional vendors that now deliver their IAM product suite from the cloud, as well as a number of new and pure cloud players. Gartner estimates that **by 2021, IDaaS will be the majority of new IAM purchases**, up from less than 20% today.

The concept of IDaaS is closely related to that of the cloud access security broker (CASB). A CASB can be defined as a security policy enforcement point, either on-premises or cloud-based, that is placed between cloud service consumers and cloud service providers. Many modern IDaaS solutions include the functionality of cloud access security broker (CASB) or can be easily integrated with it.

A more specific area of identity & access management is consumer identity & access management (CIAM). In a way, CIAM can be explained as identity & access management that is combined with processes that are similar to those of customer relationship management (CRM), such as interacting with customers, business development and managing sales and marketing campaigns. In many cases, it will be beneficial to integrate the CIAM environment with the CRM environment, so as to make it possible to gather additional information about the customers and to analyse their behaviour. In this way, services can be more tailored to the consumers' needs, and businesses can explore the full potential of sales and marketing activities when using a CIAM system, than using a CRM alone.

To a large extent, consumer IAM systems provide the same functionalities as traditional IAM environments, be it on-premise or as a service. The big difference is that the identity information of consumers comes from a variety of sources that are for a large part unauthoritative. Probably, only a small number of customer identities will be delivered by the CRM environment. The identity of these consumers has been verified and known by the organization. In reality, most customers will register themselves on the organization's website or will use the social network as an identity provider. This poses significant challenges to the veracity of those consumers' identity. As long as the services offered by the organization have a low risk profile, there is no much need to know the true identity of the customer.

As soon as more risk comes into play, however, more assurance about the true identity of the customer is required. This can be achieved by various identity proofing methods and services, such as retrieving information from third parties and asking the consumers to provide more information about their identity. Financial service providers and their regulators have long been familiar with this phenomenon, which is in this domain known as 'know your customer' (KYC), and have put into place mechanisms to identify and verify the identity of their customers to prevent fraud, money laundering and terrorist activities, as well as to detect anomalous transactions. ➔

Identity & Access Management, Identity as a Service or Customer Identity & Access Management?

The market for IAM, IDaaS and CIAM is highly volatile, with more players than ever before. Organizations that are considering any solution should carefully explore the market and thoroughly inventory and analyse their exact current and future requirements, including commercial, regulatory, functional and technical requirements. Based on this effort, an IAM architecture can be drawn and the product and service selection process can be started.

About Rob van der Staaij

Dr. Rob van der Staaij CISSP, CCSP, CISA, CISM, CRISC, CEH, CPT is principal at INNOPAY and lecturer Cybercrime & Cybersecurity at the University of Groningen. His main fields of expertise are Cybersecurity and Identity & Access Management.

About INNOPAY

INNOPAY is an independent consulting company, specialised in online payments, digital identity, e-business and cybersecurity. We help our clients, including financial institutions, governments and corporates, to develop the compelling strategies and digital services for consumers and companies that are key for successful competition in a rapidly digitising world.

Digital Onboarding – Identity Is the New Money

Innopay

Turning AML into a Competitive Advantage

Scale necessity for European banks – AMLD a blocking issue?

With Bigtech companies pounding at the gates, traditional banks and other financial service providers are challenged to slash costs while improving the service quality. However, when doing so, they face significant regulatory obstacles. Take the recently updated European Anti-Money Laundering Directive ('AMLD'), which has led to widely different interpretations across countries and deep implications for products and operations. Consumers in different regions are used to and expect certain identifying and verifying protocols, as well as, familiar authentication and signing methods for making transactions. This variety complicates things, as services also need to be tailored to local tastes. Moreover, these requirements contain a hidden competitive advantage. Not only banks have to comply with AMLD4, but so do potential newcomers. For banks this is a known fact, as they have deep experience in offering compliant products and services. For tech giants, this is a new game altogether. Key question for banks and other incumbents is how to turn this potential roadblock into an advantage: how to realise European roll-outs that are (a) compliant and (b) in line with local customer expectations?

The INNOPAY approach to geographic expansion with AMLD compliant products

In solving this complex problem, INNOPAY has developed an approach in four phases (Figure 1).

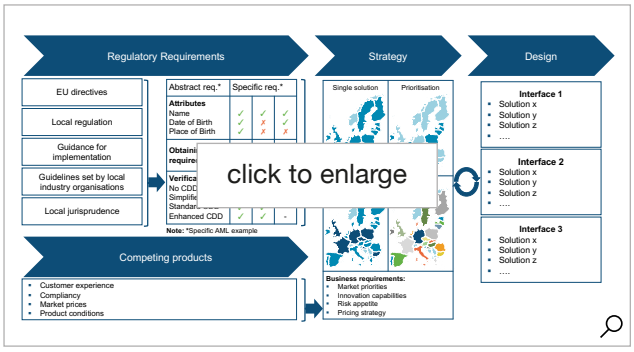


Figure 1: steps and illustrative example to assess front-end product design for AML regulation

1. Determine strategy

Product vision and strategy are key starting points for strategic decisions on product design. Decisions on strategy have to be made in developing and implementing a simple and seamless customer journey. There is an inherent trade-off between offering a uniform product across geographies and tailoring a product to local requirements in each country. The latter allows for designing an optimal product for each geography given regulatory requirements and customer expectations, but may increase cost and complexity. A second trade-off exists between being a market lead or following competitors in specific countries on specific product characteristics and product prices.

2. Analyse regulatory requirements

The first step towards realising compliant products across the footprint is assessing compliance requirements in relevant countries. This results in an overview of regulatory requirements per country. Sources for compliance requirements include EU directives, local regulation, guidance for the implementation in the local regulation, guidelines set by local regulators and local jurisprudence.

3. Analyse competing products

Analysing competing products in different countries helps in creating compliant products and gives insights into customer expectations. Market players are usually bound to offer products that are aligned to or improve on market practices to create market traction. Market practices for the customer journey differ highly across countries and regulatory requirements and existing market solutions dictate the possibilities for design.

Another reason for analysing the competitors' products is that interpretation of local regulation may result in different requirements than expected. Interpretation of regulation is best assessed in practice.

4. Determine product design

During product design, the best way to meet different regulatory regimes should be defined. However, different solution designs can all meet the same regulatory requirements. Selecting the right design should be an iterative process between product vision and strategy, customer expectations and regulatory requirements. →

Walter Lutz — *Project manager* Innopay

Jorrit Penninga — *Consultant* Innopay

Bernd Brinkers — *Consultant* Innopay

About Walter Lutz: Walter is project manager at INNOPAY and supports clients operating in transaction markets to solve strategic challenges when introducing new products or entering new markets.

About Jorrit Penninga: Jorrit holds a master's degree in Systems Engineering, Policy Analysis and Management and has experience in strategic assessments and market research on introducing innovative products and services at INNOPAY.

About Bernd Brinkers: Bernd's background in service design and experience gained at INNOPAY enables him to help clients combine technology, regulation and business value into user-centred products and strategies.

About Innopay: INNOPAY is an independent consulting company, specialised in online payments, digital identity and e-business. We help our clients, including financial institutions, governments and corporates, to develop the compelling strategies and digital services for consumers and companies that are key for successful competition in a rapidly digitising world.

www.innopay.com

Share this story

innopay

Standard Customer Due Diligence (CDD) requires the obliged entity to obtain customer attributes, the ID copy and identity verification. However, multiple solutions exist for different requirements, but not all solutions are appropriate in all cases. For a uniform product across countries, authentication through a third party identity scheme is insufficient as third party schemes are only available in some countries. The most basic customer journey, that of filling in datafields and physical verification, is not sufficient to become a market lead in a specific country.

This shows that choosing the right solutions depends on the chosen strategy. It is an iterative process between strategy development and product design. An organisation and customer experience specific optimum balance should be found.

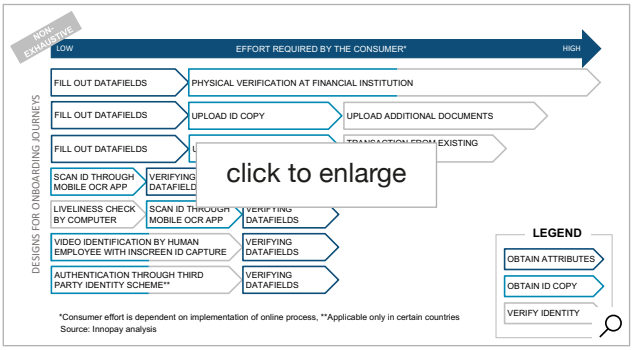


Figure 2: possible design of obtaining attributes, ID scan and verification

Towards cross-border compliant products

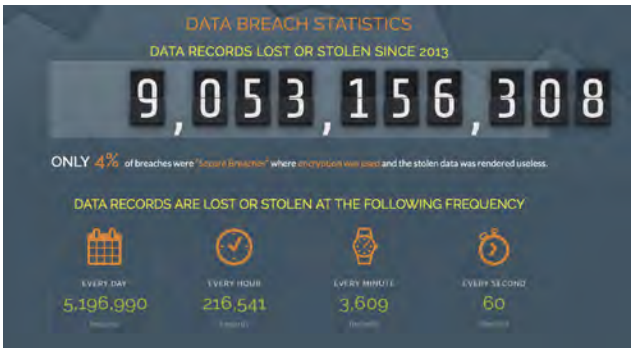
With a focus on the front-end design of financial products, geographical expansion with compliant products should be done by performing an analysis on regulatory requirements for AMLD in EU countries. Analysing competing products helps in creating a competitive product in each country, but also for interpreting regulations across countries. By expanding across geographies, traditional financial services companies will make an important step in remaining competitive in the face of the increasing competition from digital newcomers. Is your organisation ready to meet the Bigtechs challenge? Do you want to let AML work for you when driving your geographical expansion? Please feel free to contact us for more information on how to develop and deliver compliant financial service products as part of your geographical expansion strategy.

Innovate Identity

KYC is Dead – We Need to Think Differently

Know Your Customer, as we know it, is dead, and if it's not dead it's certainly teetering on the brink of death. Since 2013, over 9 billion data records have been lost or stolen and I'm sure that by the time you read this article that number has already increased.

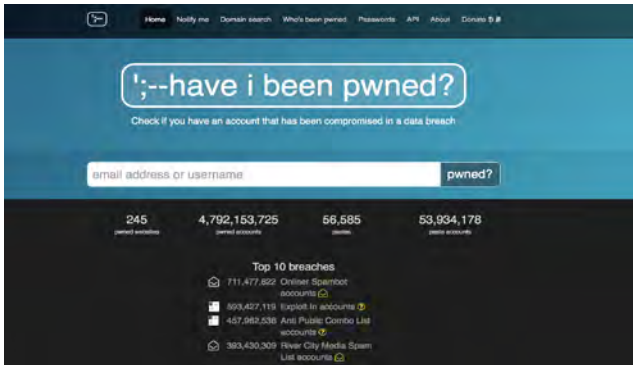
Many KYC systems are based on data like names, addresses, DOB, social security numbers. This approach to KYC has been acutely exposed with the Equifax breach, with 1 in 4 Americans now facing the danger that personal data they use to get access to financial services products are now potentially in the hands of some nefarious fraudster.



The harsh reality of online breaches

Now, when I speak to folks about data breaches, they often say "well, that doesn't affect me", but honestly, I'm not sure if they know that it does affect them. A simple check on **I have been pwned website** often shocks people, granted it's "only" an email address. Still, we all know that by using an email address the "would-be fraudster" sends out malicious links, asking us to download something, open a document or something similar so they can gain access to more personal data, which they use for social engineering and so on… until they get access to value, whether that be cash or something else.

How recent prominent data breaches come to a (likely) litigious conclusion will be interesting. In Europe, the question "who do you sue" will certainly have all eyes focused on the rollout of GDPR.



Throw in some open data initiatives, like Open Banking, PSD2 and others, and the game changes again. We create a highly competitive market (great) but one that now is inherently riskier for everyone.

Organisations admit that this isn't a siloed problem; if the company next to you hasn't got their act together and gets breached, they lose, and you lose. Classic game theory is playing out, and the players are recognising there is a lot to lose in this non-zero sum game, but also a lot to gain – and potentially there are areas of collaboration rather than competition. And, guess what, that might be better for everyone.

Organisations think there is strength in numbers

There are movements in many markets towards creating networks or schemes, like the payment schemes Visa and Mastercard, but for identity. These schemes are focused on technology and security, but also on the legal, commercial, cultural, and ethical issues to make it easier for the customer to manage identity processes, and enabling a more secure and improved customer experience.

We have seen this for some time in the Nordics, where the banks some years ago figured out that by collaborating around the issue of identity attributes and KYC they might have something to gain. Anecdotally, we know that banks participating in BankID benefit not only from the reduction in cost of KYC, but also experience an uptake in product usage by the consumer and lower abandonment rates, as they get to the financial services product faster without a break in the journey due to an "off" experience with KYC. →

Emma Lindley

Director
Innovate Identity

About Emma Lindley: Emma has been a leading industry voice in identity since 2003. As director at Innovate Identity, she acts as an independent advisor to many global brands, enabling identity as part of their digital transformation strategies. She also holds several board level advisory roles, including for the Open Identity Exchange.

About Innovate Identity: Innovate Identity is an award-winning business with a highly experienced team of digital transformation consultants specialising in online identity, security and privacy.

www.innovateidentity.com

Share this story

Collaborative approach in other regions

In Canada, there is the **Pan-Canadian Trust Framework**, a public-private partnership focused on creating a user-centric identity scheme; in Belgium, **Itsme**, where mobile operators collaborate to provide an authentication service; in Germany, **Verimi**, where Lufthansa, Deutsche Telekom, and IT company Bundesdruckerei have recently joined the initiative set by Allianz, Axel Springer, Daimler, Deutsche Bank, Postbank. In Spain, we have the Alastria consortium, which is working towards the development of a permissioned, digital ID. Then there is work in the **Decentralised Identity Foundation** amongst Sovrin, uPort and others.

At a national and international level, individual organisations realise that, despite the fact that "identity" isn't part of their core product offering, unless they do something to improve it, they and others stand to lose. They are realising that current individual approaches to solve the issue means just throwing more technology at the problem and this is not going to fix it.

As Einstein said, the definition of insanity is doing the same thing again and again and expecting a different result.

The challenge to solve the online identity crisis is an enormous one. For big problems, we need to do something different, to think differently and work together.

Holland FinTech

Digital Onboarding and KYC: Aligning the Interests of Consumers, Businesses and Regulators

Regtech is booming and many regtech solutions focus on digital onboarding and meeting Know Your Customer (KYC) and Anti-Money Laundering (AML) requirements. Who do these solutions benefit and how?

Solutions that assist with digital onboarding present significant benefits to consumers, businesses, and regulators alike. For consumers, it reduces the bureaucracy involved in signing up for financial services, thereby saving time and effort. For businesses, digital onboarding means less expenditure on customer service staff and retail space. Regulators are the drivers of KYC/AML procedures and also the main benefactors. The business systems set up for digital onboarding also assist in the flow of KYC data from businesses to regulators.

Despite these shared benefits, the interests of consumers, businesses, and regulators do not always align. KYC legislation is not harmonized in Europe. This creates problems for Financial Service Providers (FSPs) who complain that regulations are opaque or contradictory, making it difficult to offer digital onboarding services that are both compliant and consumer-centric. And for consumers, who favour ease of use, the process of fully digitizing onboarding is far too slow.

How can we better align the interests of consumers, FSPs, and regulators? To identify the pain points, we examine the relationships between these parties and the processes flow involved.

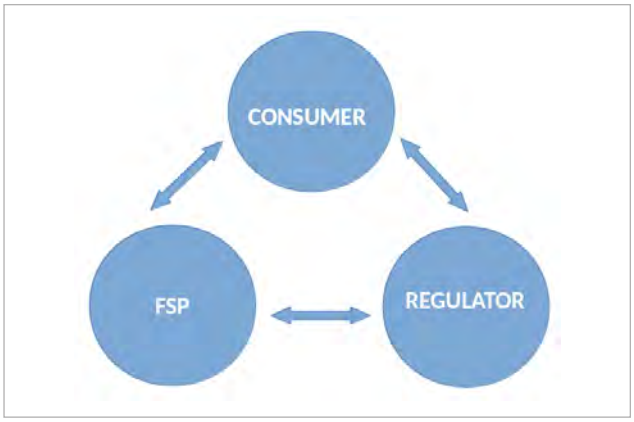


Figure 1: The relationships between consumers, financial service providers and regulators.

Digital onboarding

The process of onboarding begins when a person applies for a financial product or service. This is also the stage at which the divergent interests of consumers, FSPs and regulators become apparent.

In the Netherlands, a complete digital onboarding is still not possible for many types of financial services. Most banks allow customers to begin the process of opening a bank account online, but the procedure for completing the process varies. In some cases, banks can send an identification team to the customer's home address to spare them a branch visit. Some Dutch FSPs use derived identification in which a verified bank account can be used to prove identity.

However, digital onboarding is possible with the new generation of online banks that have emerged in recent years, such as the German mobile-based bank **N26** and the Dutch bank **Bunq**. For the new generation of financial services, digital onboarding is key to growing a client base. Rates of account switching tend to be low (see **UK figures**), even where government **regulations** have been developed specifically to encourage consumers to switch banks.

To capture a market share, new financial services must convince consumers that they offer something different from the incumbent banks, and provide a sign-up process so effortless that consumers undertake it with very little thought. If "sign up to a new digital bank" lands on a consumer's to-do list, there is a very real danger that they will never get around to the task. New financial services need to take consumers from "interested" to "converted" immediately, and a fully digital onboarding experience is key. ➔

Erin Taylor

Senior Researcher
Holland FinTech

About Erin Taylor: Erin is an economic anthropologist specializing in research into financial behaviour. At Holland FinTech she is responsible for developing a research program that serves the collective interests of the financial ecosystem in the Netherlands and beyond.

About Holland FinTech: Holland FinTech connects over 330 member companies from across Europe to our fintech knowledge base and our fintech network. We believe having access to innovative financial services and fintech solutions can empower people and organisations to understand, overview and improve their economic circumstances.

www.hollandfintech.com

Share this story

HOLLAND FINTECH

Know Your Customer

However, a complete digital onboarding is still not possible in many circumstances. Onboarding corporate clients is even harder, particularly due to the effort required to enact anti-money laundering processes and the necessary research into Ultimate Beneficial Owner (UBO). But there is hope. Regtech has been used to reduce the impact of due diligence requirements on the customer onboarding process and it could help with identifying corporate structures and assessing ownership.

Many regtech solutions are now provided by startups, either working alone or in collaboration. According to research by CB Insights, from 2012-2017, venture capital funding of regtech start-ups **totalled** approximately USD 2.3 billion. Let's Talk Payments provides a useful **overview** of some key companies providing regtech solutions in Europe. Easily missed are the parties that do not use the term regtech: often, middle sized professional services or technology companies are overlooked, such as **Figlo** and **Topicus**.

Regarding the Netherlands-based regtechs, Let's Talk Payments lists **BWise** (software solutions for risk management, internal audit, and compliance), **Open Risk** (training and risk analysis tools to the broader financial services community). **OSIS** (credit risk analysis). **ComplianceWise** and **DPA Compliance & Risk**, who both provide compliance software, are also worth mentioning.

The future of digital onboarding and KYC

Of course, digital onboarding and KYC are much broader than regtech. Consumers continue to demand human contact for onboarding in many financial services. But for businesses and regulators, regtech solutions are likely to grow in importance, given their ability to reduce costs and enable businesses to cope with changing regulations. In this way, they help to better align the interests of consumers, businesses and regulators.

Digital Identity –
Creating Identity Hubs

EEMA

The Role of Financial Institutions in Delivering Identity-as-a-Service for Governments

Why financial institutions make good identity service providers

In many countries, banks engender similar levels of trust to governments. In some countries they are even more trusted, with citizens investing their savings with banks or financial institutions, and many companies using banks as funding sources.

Trust

Trust itself is not binary, and the role of regulatory bodies and guarantee schemes is to help investors and borrowers keep faith. Banks and financial institutions are also protected, as they are forced into anti-money laundering (AML) and Know-Your-Customer (KYC) checks, which reduce and help quantify risk and maintain regulatory compliance. This circle of trust, powered by regulation and risk management, helps with keeping the symbiotic relationship between financial institutions and their customers. This is not similar when it comes to citizens and government, their relationship being somewhat different, with little perceived accountability and transparency. Banking regulation contributes to the Levels of Assurance (LoAs) for credentials and transactions, which can be partially mapped on to governmental LoAs determined by legislation (such as eIDAS), therefore bridging the gap between government and the finance sector, and enabling cross-purpose use.

Finance

Identity programmes need substantial take-up in order to be financially successful. That is precisely why governments prefer to use banks (among other financial institutions) as IDSPs. In developed countries, banks already have a relationship with a majority of the population, and these are coupled with KYC and AML checks. This means that the cost of enrolment may be shared with the normal financial onboarding process, thus saving substantial amounts of cost. Additionally, current authentication methods can often be re-used.

Contract

Governments are bound by rules set down by legislatures and agility is not always possible. Financial institutions, on the other hand, can have a contractually-based relationship with their customers. Service level agreements, liability caps and enhanced services such as insurance can all be offered, plus service differentiation between multiple IDSPs.

Architectures for Identity Service Providers

Direct and Derived Models

Direct Models are typical of the more basic schemes and were used by countries such as Austria, Estonia and Belgium. These schemes are based on smartcards primarily and the government acts as the IDSP. However, these have been recently utilising derived eID's to overcome the legislative problems of mass mobile device usage, with an IDSP serving a secondary eID and using the original government eID as a major component in enrolment.

3-Corner Model

This is used by countries such as Denmark (NemID) and the Netherlands (DigiD). Here, the government contracts a third-party IDSP to provide enrolment and authentication. In the case of NemID, it also includes digital signing and the entire scheme was built and operated under contract.

Hub Model

This model is similar to the 3-Corner Model, except that the government owns and/or operates a hub(s), which accept(s) identity assertions from multiple accredited IDSPs. In the UK's case, a user can have an enrolled identity in each IDSP. The hub acts as an air-gap between the IDSPs and the services, so that the IDSPs do not know which services are being used. Additionally, as there is no national registry, the Minimum Data Sets are relayed for each service provider to map the identity asserted to an existing user record. Germany has three private-sector owned hubs with associated IDSPs. Canada uses a single privately owned hub, accommodating private authentication (only) providers and an alternative government digital identity credential.

4-Corner Model

This is a more sophisticated model where counterparties with different IDSPs can interact through a hierarchy of trust, leading to a common 'trust root'. In Norway's case, it is owned by The Norwegian Financial Services and Saving Banks Associations. ➔

Jon Shamah

Chair
EEMA

About Jon Shamah: Jon Shamah is the Chair of EEMA. He is a recognised international digital Identity & Trust Subject Matter Expert, specialising in maximising the operational value chain of national eID schemes. He is a frequent public speaker on issues surrounding identity, Trust and EU Trust Services regulations and contributes to European Programs such as FutureTrust and LIGHTest.

About EEMA: EEMA is the leading, not for profit, independent European think tank including topics on identification, authentication, privacy, risk management, cybersecurity, the Internet of Things, Artificial Intelligence and mobile applications. EEMA helps organisations maintain their competitive edge through projects, world-class events and European business networking.

www.eema.org

Share this story

In this model, the government portal is one of the many relying parties.

Examples of Banking Implementations

NemID Denmark

NemID was chosen in 2010, and it is operated in a private-public partnership between NETS and the Danish government. It is server-centric and was originally TAN (Temporary Authentication Number) card based, but now uses mobile OPT (One Time Passwords). NemID can be used for bank access as well as business and eGovernment services. It is used on average once every three days by every citizen. NemID will be connected to the Connecting Europe Facility through Denmark's eIDAS node for mutual recognitions across the EU.

BankID Norway

With the large number of Norwegian banks, the need for a common method of authentication resulted in BankID, formed and operated by BBS (now NETS). In 2014, there was an agreement between BankID and the Norwegian government to use BankID as authentication for eGov services accessible through the government's portal. BankID still maintains usage of about 1.4 million authentications per day (out of a total population of about 4.5 million citizens).

Barclays Bank UK

Barclays Bank is a multi-IDSP hub and one of the certified IDSPs for UK.GOV.Verify. Barclays Bank uses its enrolment and registration systems to supplement its own bespoke UK.GOV.Verify systems to provide a rich registration and strong trust branding. A minimum data set, determined by the UK government, is transmitted together with the identity assertion to enable the matching with the various UK government agencies, as there is no central registry in the UK.

Conclusions

Financial institutions, and banks in particular, are ideally placed to become the IDSPs of governments, and whilst it may not be the only business sector able to fulfil the role, they have an advantage due to their regulated environment and risk management philosophies.

Kapronasia

Aadhaar Unique IDs in India: A Qualified Success?

The Digital India project initiated by the Government of India has made significant headway in the last few years. As part of this project, the Unique Identification Authority of India (UIDAI) has presided over the allotment of unique identification numbers to all Indian residents since 2009. Currently, more than 1.1 billion Indian citizens and residents have Aadhaar IDs, making this the largest exercise of this kind the world has ever seen. There are many potential benefits of such a scheme, but there are also concerns and pitfalls. Besides the advantages, this article also focuses on some of the security and privacy concerns related to Aadhaar, which are often overlooked.

Benefits of Aadhaar

India is the second most populous nation on earth, with more than 1.3 billion people. Having a unique identification system in place would be a fillip for the government, as it would allow government schemes for poverty alleviation and improvement in health and educational well-being to be better targeted. For example, if a needy person's bank account is linked to their Aadhaar biometric ID, then it would be easier for the government to provide funds to the individual without using any intermediary. In a country struggling with corruption throughout the government machinery, being able to reach the target audience directly is a significant benefit. Similarly, if both the bank accounts and the tax IDs of individuals are linked to the Aadhaar ID, then the government can trace the income and expenditure of its citizens, thereby obtaining vital information that would allow it to counter money-laundering and the shadow economy.

Security challenges are paramount

Creating a monumental technology infrastructure to meet the requirements of a population of more than 1.3 billion people does not come without its problems. Many people have questioned the wisdom of concentrating so much critical personal information in a government platform that is not known for having a robust security framework. There have been two prominent instances in which the Aadhaar database has been compromised.

In May 2017, the Bengaluru-based Centre for Internet and Society (CIS) alleged that there had been an illegal breach of the database, and Aadhaar identity numbers of more than 130 million people had been leaked online, along with their dates of birth, addresses, and tax IDs (PAN). It is believed that the revealed information did not include the biometric identification of the people affected, but the breach was significant nonetheless as it exposed millions of people to possible fraud.

The response of the UIDAI was also insightful, because it asked the CIS to reveal on which servers the data was stored, and who might have been responsible for the breach. The UIDAI response quoted the relevant laws, namely sections of the Information Technology Act, 2000 and the Aadhaar Act, underlining the liability under law. The aggressive approach of the UIDAI forced the CIS to retract some of its claims, but then the focus of the discussion was shifted from the loss of critical information to the semantics of the claims of CIS. Instead of calling the breach a "leak", after receiving the letter from UIDAI, CIS stated that it was merely an "illegal disclosure".

The second instance of a breach occurred between **January to July 2017**, when an IT expert hacked into the Aadhaar-enabled e-hospital system created under the Digital India project of the Government of India. His intention was to access the central identities data repository of UIDAI for verification of Aadhaar numbers, to be used for an 'eKYC Verification' app created by him. The UIDAI database gave him access considering that it was the e-hospital system that was requesting the Aadhaar identity verification. The hack shows that the security protocols of the UIDAI require significant overhaul before it can be trusted to protect the hundreds of millions of digital identities in its database. →

Anshuman Jaswal

Director, Capital Markets and Head of Indian Financial Services

Kapronasia

About Anshuman Jaswal: Dr. Anshuman Jaswal is Director, Capital Markets and Head of Indian Financial Services at Kapronasia. He has extensive research and consulting experience, and has written more than 100 reports on a variety of topics in financial services.

About Kapronasia: Kapronasia is a leading independent research and consulting firm focused on the Asian financial services industry. We help financial institutions, technology vendors, consultancies and private equity firms understand the impact of business, technology, and regulatory issues on the banking, payments, insurance and the capital markets.

www.kapronasia.com

Share this story

kapron ASIA

Aadhaar and the right to privacy

The Indian constitution does not mention a right to privacy. This has been raised as a serious concern by the critics of Aadhaar, since there is no related privacy framework that outlines how the government can use the Aadhaar information. However, the Supreme Court of India addressed some of these concerns when it held, in August 2017, that privacy is a fundamental right under the Constitution with reasonable restrictions. It was a landmark decision in the Indian context, since it could affect the way in which the unique identification data is collected, and especially the means for which it is used. For example, in the past, the government has mandated that Aadhaar data be linked to citizens' information from bank accounts, tax filings, medical records and phone numbers. Once this is achieved, the government would have unregulated access to such information. There is currently no statute or legal precedent to guard against abuse or to allow an individual to file a complaint.

The Supreme Court decision gives encouragement to citizens and institutions that are concerned about the rights of ordinary individuals, while also laying the groundwork for further work that needs to be done to create a robust legal framework in this field.

Online Authentication – Customer Experience is Crucial

Easy Solutions

Ricardo Villadiego, Easy Solutions CEO, considers that businesses nowadays face a dilemma – how to protect customers from increasingly sophisticated cyberattacks without the hassle of overly complex login methods. The mobile phone has already brought to users instant gratification, making them totally reluctant to any inconvenience that some security products may require. In spite of this, biometric technology can now integrate the customers' individual physical attributes, including their fingerprints, voice and facial features, into every company's authentication strategy.

Account takeover causes now more than USD 7 billion in losses per year. What needs to be done to protect banks, ecommerce companies and their customers?

Account takeover occurs when a fraudster is able to obtain personal information and gain unauthorised access to a customer account. This can happen for any type of online account, including financial, email, social media or online retail accounts. Often phishing and malware are used to steal this information.

> *"Companies employing a multi-layered fraud security strategy that addresses threats at every stage of the attack lifecycle have the best way to thwart fraud.*

Cybercriminals have become particularly adept not only at breaching the security systems of large companies, but also at breaking into the online bank accounts of individual internet users. There is no magic 'silver bullet' to stop all fraud, but companies that employ a multi-layered fraud security strategy that addresses threats at every stage of the attack lifecycle have the best way to thwart fraud. The critical components of a multi-layer anti-fraud strategy include: proactive monitoring of external threats, online navigation protection, user authentication and user behaviour analytics.

Since you mentioned biometrics, could you please explain what the main benefits of this technology are?

Biometric authentication technology is likely to be a game-changer. It uses the unique physical characteristics of an individual and is increasingly being employed as a way to confirm online purchases, payments, and bank transactions. Next-generation biometric fingerprint, facial, and voice recognition technology is highly secure, and best of all, it's easy for customers to use and doesn't require them to memorise a username-password combo or input a business-transmitted passcode. Nevertheless, like any other authentication solution, biometrics is most secure when coupled with other authentication layers, like push notifications, one-time passwords, QR-codes, device identification and more.

How is biometric authentication superior to other kinds of end-user authentication solutions?

For the average customer, there is always a need of a balance between security and ease-of-use. Some other authentication systems are highly secure, but are rigid and require the user to follow many steps before they can log in or make a purchase or transaction. This leads to frustration so users avoid using the security because it's so inconvenient. If a user authentication system is too lenient, it's liable to be compromised by hackers. Biometrics strikes this balance naturally, as it is highly secure, extremely difficult to crack, and easy to use. It's also better than some types of one-time passcode (OTP) authentication; SMS-delivered OTPs, for example, are vulnerable to capture by cybercriminals. And, of course, biometrics is by far a better authentication system than the old username/password combo.

What would you say to an organisation that is considering adopting biometrics as part of their current security strategy?

I'd say that they're quite a forward-thinking organisation. It's definitely a good idea to do your research, as there are a lot of different types of biometric systems that are meant to secure different things. Also, it's a good idea to audit their current user-verification system, and ask: is it as secure as it could or even should be? Have there been breaches in the past? How have compromised customers reacted? ➔

Ricardo Villadiego

CEO
Easy Solutions

About Ricardo Villadiego: Ricardo Villadiego is the CEO of Easy Solutions, a Cyxtera Business and leading provider of fraud detection and prevention solutions to financial institutions and enterprises around the world. Villadiego has spent the last 20 years helping organisations to overcome electronic fraud challenges under a holistic vision: Total Fraud Protection.

About Easy Solutions: Easy Solutions is a security provider focused on the comprehensive detection and prevention of electronic fraud across all devices, channels and clouds. Products range from digital threat protection and secure browsing to multi-factor authentication and transaction anomaly detection, offering a one-stop shop for end-to-end fraud protection.

www.easysol.net

Click here for the company profile

Share this story

EASYSOLUTIONS®
A CYXTERA BUSINESS

Or perhaps their current user authentication system is highly secure but is a hassle to use it. If companies want low-friction security for their customers, then, I'd say, biometric authentication is right up their alley.

What do you predict that future of fraud will look like?

It's not easy to predict the future, but within our lifetimes, I think that both fraud security and online commerce will be barely recognisable when compared to the way they are today. Biometrics has the potential to make things that we're used to – credit cards and logins, for example – obsolete. What if you could log into an account with a touch of your fingerprint, make a transaction simply by saying it, or purchase items by taking a 'selfie' photo? That might be what the future holds. And the next generation of hackers, like their forefathers, will use all their ingenuity to find and exploit system weaknesses, however slight or small those weaknesses may be. But, just as the digital transaction systems of tomorrow will be more able to detect, block, and neutralise the most potent of fraud attacks we know of today, fraudsters themselves will innovate, and other, more advanced attack methods are likely to emerge. What those attack methods are, could be anyone's guess.

Aite Group

The Customer Journey in M-Commerce Checkout: How to Navigate Security Roadblocks

Payment management is becoming strategic for ecommerce. Merchants are striving to streamline the customer journey as much as possible to convert more customer visits into sales. A seamless payment experience is essential to achieve that. At the same time, however, card-not-present (CNP) fraud has been rising at a rate commensurate with the growth in ecommerce as a whole.

Regulators around the world are mandating secure customer authentication (SCA) to protect consumers from online fraud. In Europe, the PSD2 requires payment service providers (which include banks, e-money providers, and payment institutions) to apply SCA for all electronic payments initiated by the payer (such as card payments and credit transfers) above EUR 30, unless the payment qualifies as low risk. So how to balance the demand for a "click and pay" experience with the requirements for secure payments?

Mobile commerce requires a seamless user experience

Fraud prevention techniques often require step-up authentication e.g., via a one-time password, introducing friction in the check-out process. This tension between security and customer experience has been aggravated by the rise of mobile commerce. The mobile customer, while on the move and working on a smaller screen, has even less tolerance for security methods that make the checkout process inconvenient and clunky.

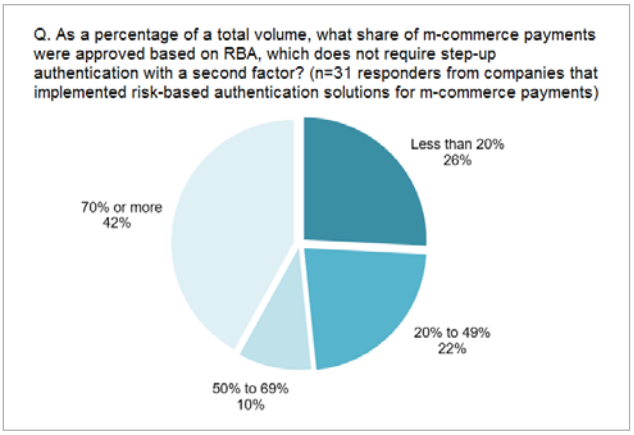
A recent survey that Aite Group and Mobey Forum conducted (see the report: **Authentication in M-Commerce: Balancing Risk and Experience**, November 2017) confirms that the user experience is considered to be the most important criterion for merchants when they evaluate their approach to payment transactions.

Risk based authentication: best of two worlds

Payment companies have found a solution for the customer experience versus security conundrum in risk based authentication (RBA).

With RBA, the company will test the transaction against a series of parameters in real time—e.g., the device used by the customer, the IP address, the location, and the typical behaviour of the customer. If no anomalies are found, the transaction can be approved without invoking step-up authentication, allowing a smooth payment experience for the majority of legitimate transactions. As it comes to the effectiveness of RBA, almost half of the survey respondents that implemented RBA solutions said that 70% or more of m-commerce payments were approved without requiring a second factor (Figure 2).

Figure 1: Effectiveness of Risk-Based Authentication



Source: Aite Group and Mobey Forum online survey with 76 executives (November 2017)

So RBA works well in practice, but how does it fit in with the PSD2 SCA requirements?

PSD2 allows for RBA exemption

The PSD2 has included an exemption for the application of SCA that allows PSPs to implement RBA (called "transaction risk analysis") under certain conditions. The amount, or "exemption threshold value (ETV)", that it applies to depends on the PSP's fraud rate for remote card-based payments and credit transfers, respectively. The maximum ETV is EUR 500 (see Table 1). ➔

Ron van Wezel

Senior Analyst
Aite Group

About Ron van Wezel: Ron van Wezel is a senior analyst for Aite Group's Retail Banking & Payments practice. His research covers market and regulatory trends in the payments space, with a focus on Europe.

About Aite Group: Aite Group is an independent research and advisory firm focused on business, technology, and regulatory issues and their impact on the financial services industry. Headquartered in Boston, Aite Group works with its clients as a partner, advisor, and catalyst, challenging their basic assumptions and ensuring they remain at the forefront of industry trends.

www.aitegroup.com

Share this story

Aite

Table 1: SCA Exemption Using Transaction Risk Analysis

ETV	Reference fraud rate for remote card-based payments	Reference fraud rate for credit transfers
500 euros	0.01 %	0.005 %
250 euros	0.06 %	0.01 %
100 euros	0.13 %	0.015 %

Source: European Banking Authority (EBA)

The lowest reference fraud rate for remote card-based payments of 0.13% seems achievable for PSPs. In 2016, the UK reported an average ecommerce fraud rate of 0.124%, suspiciously close to the lowest threshold in the EBA's table (see: **Fraud the Facts 2016: The Definitive Overview of Payments Industry Fraud**). That would mean that the threshold for (mandatory) multi-factor authentication can be raised to EUR 100, well above the average value of ecommerce transactions (EUR 67).

Online stores selling high value products (such as electronics stores, or travel agents) would still be required to apply multi-factor authentication for a large share of their transactions. But perhaps the issue is a temporary one. Consumers may get used to SCA over time, as all PSPs and merchants will have to apply it. New techniques such as biometric authentication could reduce the burden of SCA, at least for the m-commerce environment. Respondents to the survey appeared to have mixed opinions on this issue, but only a minority thought that SCA will have high impact on merchant sales.

Conclusion

Merchants are advised to work with the best PSPs to reduce their average fraud rate and make use of the exemptions that the PSD2 provides for RBA. Still, more transactions will require SCA under the PSD2 rules, but as consumer behaviour adjusts to its use, and new techniques such as biometrics reduce the friction, merchants will be able to keep their customers happy with a seamless and secure check-out experience.

FIDO Alliance

Modern Authentication: The Key to Achieving Security, Usability and Regulatory Compliance

As banks, online services, regulators and technology providers look to revamp authentication to better address today's challenges, an unprecedented rate of disruptive innovation and regulatory change is taking place. From the availability of modern authentication solutions to new regulations, the identity management space may seem complex to navigate, but it also provides a lot of opportunities.

Out with the old...

We are in the midst of a burst of authentication technology innovation. As a result, some of the methods that we have depended upon for authentication should now be sorted into the "old" column for methods to move past. The first on that list is single-factor passwords. One needs to read the many recent headlines to know that passwords are at the heart of the data breach problem. According to the **Verizon Data Breach Investigations Report**, 81% of data breaches in 2016 involved weak, default, or stolen passwords, up from 63% in 2015.

In the identity space, the idea of using two-factor authentication is a well-established mitigation for replay attacks using stolen passwords. However, even the most commonly used "strong authentication" methods have issues that have prevented their widespread adoption and therefore belong in the "old" column.

This includes one-time passwords (OTPs) delivered via text messaging or email. This method ranks low for usability: users get frustrated with having to deal with multiple screens just to log into their accounts, and reliability of SMS delivery cannot be ensured; as a result, opt-in rates for this method are low. On the security side, OTPs are still vulnerable to social engineering and phishing.

Smart cards, also a legacy method, do offer strong cryptographic security, but are inconvenient to use, costly to implement and don't support the current mobile/BYOD environment in the workplace. This is more problematic than ever before given the growing demand for secure access to heterogeneous cloud services.

… and in with the new

New, modern authentication solutions are based on FIDO Alliance standards. FIDO Authentication takes advantage of the biometric capabilities in devices that most consumers already have, or of the increasingly popular "security key" second-factor devices, and adds interoperable protocols for strong cryptographic authentication. FIDO standards provide the ability to offer multi-factor authentication based on public key cryptography using the same device (like biometrics in a mobile device and security keys) across services. Many organisations, especially banks, are considering biometrics in particular as a good option to improve the user's authentication experience. The trend is due, in part, to the fact that the majority of mobile devices are shipped with built-in biometric features like fingerprint scanners and facial recognition. These devices are also being certified to validate their ability to secure on-device storage of sensitive user data, such as private key application credentials and biometric data. With user credentials stored on the user's device and not on servers, there is no risk that criminals can re-use credentials harvested from someone else's data breach. In the FIDO model, an attacker would have to gain physical possession of a user's device to even attempt such an exploit. These types of attacks are not scalable or profitable for cybercriminals -- essentially eliminating the threat of credential stuffing and phishing. Similarly, using an on-device method to store biometric templates is the preferred approach by today's manufacturers because it / for it effectively protects online authentication systems against scalable attack.

A standards-based way to meet regulatory requirements

PSD2 Strong Consumer Authentication (SCA): FIDO standards provide a way to meet PSD2 SCA requirements while also addressing organisational and user demand for transaction convenience. While the final draft Regulatory Technical Standard for PSD2 requires two secure and distinct factors of authentication, it also recognises that these factors can be housed in a single "multi-purpose" device – such as a mobile phone, tablet or PC – as long as "separate secure execution environments" are used (such as trusted execution environments (TEE), secure elements (SE) and trusted platform modules (TPM)). ➔

Brett McDowell

Executive Director
FIDO Alliance

About Brett McDowell: Brett McDowell is the Executive Director of the FIDO Alliance, the organisation he helped establish in 2012 to remove the world's dependency on passwords through open standards for strong authentication. Previously, he was Head of Ecosystem Security at PayPal, where he developed strategies and lead programs to make the Internet safer for PayPal and their customers.

About FIDO Alliance: The 250+ member, cross-industry FIDO Alliance provides specifications and certifications to enable an interoperable ecosystem of on-device authenticators that can be used for simpler, stronger authentication to many compliant mobile apps and websites. Support for FIDO authentication has been built into flagship devices from top handset manufacturers, while some of the most trusted brands including Google, Facebook and PayPal have made FIDO authentication available to protect more than 3 billion end-user accounts.

www.fidoalliance.org

Share this story

This is already the preferred method of FIDO authenticator implementation being practiced today.

Most internet-connected consumer devices, such as laptops and mobile phones, are shipping with these already built-in security capabilities, as well as on-device biometric authenticators. This means that organisations can leverage a rapidly growing install base of laptops and mobile phones, to meet PSD2 SCA requirements by implementing support for FIDO Authentication standards in their payment applications, such as card-on-file wallet services and merchant applications.

GDPR: Guidance from **ENISA** regarding GDPR compliance suggests that organisations use two-factor authentication for accessing systems that protect personal data. Using FIDO standards and implementing strong authentication with biometrics and/or security keys are a suitable option as the standards dictate that no personally identifiable information (PII) of any kind is stored centrally. Though one may use FIDO-enabled devices across services, there is no sharing of private key credentials or device identification data with those services, fulfilling the data minimisation goals of GDPR when applied to account credentials. In contrast, other online authentication and identity technologies store credentials, including biometric data, in centralised databases where they could be exfiltrated en masse from a single data breach.

Modern authentication is the path forward

It's time for financial institutions and all organisations to embrace modern authentication as the way forward. This will lead to the widespread adoption necessary to stop the data breach problem that has been plaguing us in recent years, and to meet various regulatory requirements that have consequently emerged as a result. At the same time, it is critical to evaluate the security and privacy of the solution before adopting any new multi-factor authentication approach. Standards-based approaches like FIDO, that utilise public key cryptography and exclusively store user credentials and biometric data on the user's own personal device, aim to be a fit-for-purpose approach to get the desired security and usability while also meeting regulatory requirements.

Gropay

Strong Customer Authentication (SCA) – Action Plan for Online Merchants

By now, many European banks, PSPs, merchants and fintechs involved in the digital transaction space have heard of PSD2, and everyone agrees that one of the regulation's objective is to make payments safer and more secure.

These entities are currently waiting for the Regulatory Technical Standards (RTS) on Strong Customer Authentication (SCA) and Common and Secure Communication (CSC) to be adopted by the European Commission and Parliament.

Nevertheless, merchants are asking themselves how SCA will impact conversion, and how should they prepare themselves for the upcoming regulation.

Strong Customer Authentication (SCA) – definition and exemptions

SCA is part of a European regulatory initiative to reduce ecommerce fraud by ensuring an appropriate level of payer authentication through at least 2 of the following elements:

1. Something the payer knows: e.g. password;
2. Something the payer has: e.g. randomly generated PIN on a security device or a PIN via SMS to the payer's mobile phone;
3. Something the payer is: e.g. biometric identification like fingerprints or iris scans.

The responsibility for SCA rests with the payment service provider (PSP) of the merchant, a service paid by the payee, and the PSP of the payment instrument used by the payer. It is expected that the merchant's PSP will initiate SCA; however, if they do not, then the payer's PSP can still insist upon it.

The EBA also offers a number of important exceptions for online merchants, under which authentication will not be required:

- Small value transactions – transactions under EUR 30 will not require SCA. However, after either 5 consecutive transactions below EUR 30, or a cumulative total of EUR 100 from the same payer to the same payee, the next transaction will need SCA;
- When the payer is not initiating the transaction – recurring payments where the payee is initiating the transaction will be exempt from SCA and also direct debits;
- When the payer trusts the payee – card-on-file and one-click payments will continue to be allowed without the need for SCA at each subsequent payment;
- When either the acquirer is not based in the EEA, or the payment instrument is not issued in the EEA – merchants concerned more about conversion than fraud might choose to work with non EEA acquirers;
- Transaction Risk Analysis applied payments – the SCA rules allows PSPs to perform their own risk assessment on a transaction and choose not to apply SCA if they feel confident that the transaction is not fraudulent. However, the PSP must stay below the fraud limit imposed by a regulator to be able to enjoy this flexibility. If their fraud levels rise, then they will be forced to perform SCA.

Regulatory impact for online merchants

As PSPs begin to incorporate SCA, they should contact merchants to inform them of the coming changes. Depending on how PSPs choose to implement SCA, merchants may need to make changes to their contracts and technical integrations with their PSP.

SCA is expected to have a positive impact on fraud. In 2016, approximately **USD 16 billion was lost just to card fraud globally**. The SCA aims to reduce this loss. Reduction in fraud will give consumers more confidence to transact online and should mean that ecommerce growth can continue without friction from fraud.

Fraud, which has been monitored and regulated primarily by the payment schemes, will now be monitored by the financial regulators that license PSPs. This will give space for the emergence of new and innovative methods of payment to challenge cards, with the re-assurance that high levels of fraud will not encumber these methods. →

Manoj Kheerbat

Founder and CEO
Gropay

About Manoj Kheerbat: Manoj is founder and CEO of Gropay, an Amsterdam-based payments and fintech consultancy. Manoj is on a mission to deliver exceptional, measurable benefits and value to the 'last mile' of B2C payment delivery – the online merchant and their immediate service providers.

About Gropay: Gropay was founded in 2008 and delivers payment focussed consultancy and interim management across the globe. Gropay specialises in 4 key service areas:
Growth: Business development, global expansion, relationship management and talent acquisition
Operations: Product, risk and fraud management
Compliance: Regulatory and contractual
Mergers and Acquisitions: Due diligence and acquisition management

gropay.com

Share this story

GROPAY

Merchants who already use 3D secure (3DS) and transact predominantly in cards should not see any major impact. Some implementations of 3DS that involve a password and some form of token satisfy the requirements around SCA. However, there are many implementations of 3DS that require only passwords; these are not compliant with the new SCA requirements. Also, 3DS cannot be applied to mobile in-app payments.

The card schemes (Visa, Mastercard) are working towards a new version of 3DS that will be SCA compliant.

Merchants transacting primarily in smaller value transactions, below EUR 30 will see little impact. Merchants using card-on-file will only see the impact on the initial conversion transaction. This should make card-on-file and tokenization an essential and universal offering from PSPs.

Forcing authentication on the payment page is expected to have a negative impact on conversion. Merchants are likely to migrate to low-risk and larger acquirers, whose lower fraud levels give them the flexibility to not apply SCA.

Merchants working with acquirers that have higher risk merchants in their books may find value in switching to acquirers with a better blend of higher and lower risk transactions. These acquirers with lower fraud levels will have more flexibility to not mandate SCA and keep the conversion process friction free.

Non-European domiciled merchants with substantial EU consumer traffic may want to weigh in any advantage offered by the integration of a European acquirer against the demands that will be placed by SCA.

Merchants originating in the EEA with entities outside of the EEA may want to consider internal re-organisations to be able to transact via their non EEA entity and a non EEA acquirer.

Therefore, the work and change required to do this should be balanced against the benefit that might be gained by being able to circumvent the SCA requirements.

Juniper Research

3D Secure 2.0 to Drive Online Payment Fraud Detection Spend

The 3DS version (1.0.2), which is currently most in use, has been suffering from drawbacks, discouraging both consumer use and merchant integration:

- Poor mobile integration;
- Potential for MITM (man-in-the-middle) attacks;
- Being mistaken as a phishing scam by the end-user;
- End-users have to enrol in the service with their bank before benefiting;
- There are no standardised requirements regarding password strength, leading to passwords that can potentially be broken by brute-force.

These factors have led to increased instances in cart abandonment; however, merchants have felt that in some cases, the potential revenue loss from cart abandonment is greater than the potential loss from fraud.

The industry has reacted to these shortcomings with the development of 3DS 2.0. This new version aims to address many of the weak points seen in the previous version 1.x while also being compatible with the PSD2 requirements.

The body developing the new standard, **EMVCo**, first announced the availability of 3DS 2.0 in October 2016. Due to the need of preparation, it will undoubtedly take some time until the merchant uptake of the standard becomes widespread (for instance, there are significant regional differences in how 3DS challenges are implemented).

In European markets, approximately 90% of 3DS enabled payments do not require an authentication challenge. This is because European merchants and issuers use their own risk-based solutions to determine if a challenge should be issued.

In the US, this figure falls dramatically, with many issuers implementing a 100% challenge strategy. This ignores the potential for data points to assess risk and improve the consumer experience.

The new standard focuses on adopting a risk-based strategy, which should render 100% challenge rates obsolete.

3DS1.x vs 2.0

Source: Visa

The introduction of this feature into the standard will impact the issuers working with Visa and Mastercard, meaning that they will incorporate more cardholder data into the model. Among other information, such as the used device, time zone and so on, it will help determine the buyer's authenticity. Indeed, the ability for merchants to combine their customer data (reputation, behavioural indicators etc.) with issuer data is a paradigm shift compared to how the standard was managed before. This should dramatically improve the service in terms of its risk-based approach.

In many instances, particularly with mid- to high-end mobile devices, biometrics may be used for authentication. However, the aim is to replace static passwords, prevalent in version 1.x, with One Time Passwords.

One of the key factors in determining the spread of 3DS 2.0 will consist of how quickly do issuers respond to the new feature set. Version 2.0, for example, is not compatible with earlier versions, which means that MPI (Merchant Plug-In) providers will have to send the correct messages to the issuer depending on the latter's capabilities.

Indeed, according to **CyberSource**, even in a mature ecommerce space such as EMEA, only **80% of issuing banks adopted a risk-based approach in 2014**. This proportion has undoubtedly increased since then, particularly as machine learning solutions have been democratised over the last three years. Nevertheless, other regions will have significantly a lower proportion of issuers able to adopt a risk-based approach. ➔

Nitin Bhas

Head of Research
Juniper Research

About Nitin Bhas: Nitin Bhas is the Head of Research at Juniper Research. He joined the company back in 2010. He leads the analyst team and develops Juniper's annual and long-term research plan and product strategies. He also leads and participates in ad-hoc research and consultancy projects along with Juniper's expert team of analysts. He is a regular speaker at industry conferences and is frequently interviewed by the BBC, CNBC and Reuters.

About Juniper Research: Juniper Research is acknowledged as the leading analyst house in the digital commerce and fintech sector, delivering pioneering research into payments, banking and financial services for more than a decade.

www.juniperresearch.com

Share this story

JUNIPER RESEARCH

In effect, this means that adoption in emerging ecommerce markets is likely to be lower. In such markets, the mobile is the primary computing device, so it will be more likely to suffer fraud owing to no, or poor implementation of the old 3DS standard.

Meanwhile, there are several operational changes that must occur at various nodes in the payment channel for 3DS 2.0 to be supported:

- Payment technology providers, payment processors and gateways must work with the new specification and accompanying SDK (Software Development Kit). EMVCo has made the specification for browser and mobile app-based authentication available for download, free of charge;
- A framework for functional testing and compatibility with the new specification is still under development. The additional work by the PCI (Payment Card Industry) Security Standards Council for data security requirements, testing procedures, assessor training and reporting templates will address the environmental security that is to be completed. EMVCo expects these documents to be released in the course of 2017;
- Merchants and issuers will need to update their internal systems to ensure they are ready for the new standard. This will require some work by MPI providers as well as the third party ACS (Access Control Server) providers commonly used by issuers.

In conclusion, it will take some time until the new standard will roll out and become widely used, given that full work on the developer side is unlikely to begin before the end of 2017. Yet, Visa **estimates** that rules for merchant-attempted 3DS transactions will extend to 3DS 2.0 from April 2019.

PSD2

Juniper believes that PSD2 will have a significant impact on the speed of 3DS 2.0 rollouts within the EU. On account of its static password scheme, the current version of the standard does not comply with PSD2 demands for Strong Customer Authentication. However, through adoption of biometrics, tokenisation and OTPs, the latest version will meet the PSD2 requirements and thus it can be used as part of the Multi-Factor Authentication challenge flow.

Regulations and Directives- Opportunities, Obligations, and Obstacles

Accenture

PSD2 and GPDR – Customer Consent is (the) Key

2018 will undoubtedly prove to be an impactful year for financial services. Two major EU regulations of great importance to banks will come into force in the first half of 2018. While the **PSD2** is all about making the data of individuals available to third parties, the GDPR is all about keeping this data private. Surprisingly, little has been said in the regulations about their seemingly conflicting coexistence.

A closer look at the regulatory landscape

On the one hand, the potential penalties are huge for an institution if it fails to comply with data breach notification under the GDPR – up to EUR 20 million, or 4% of global turnover. Being a regulation, GDPR is directly applicable within all member states of the EU. On the other hand, PSD2 is a Directive, so penalties are up to the member states to define, therefore there might not even be fines for non-compliance.

In preparing for PSD2, banks should take the GDPR guidelines at heart, applying the most rigid possible interpretation. In turn, this would limit the TPPs' access to data and lead to strict interpretations of consent. It would also slow down the **open banking** movement and reduce the effectiveness of regulators' efforts to increase innovation and competition in the payments market. Banks should ensure a common framework for an aligned and coordinated approach by taking into account the requirements of both GDPR and PSD2.

Consent – common concern of PSD2 and GDPR

Both GDPR and RTS under PSD2 lack clarity on the form of the required consent. Considering that consent in electronic form is a practical necessity for PSD2, the technical means of providing consent are also lacking (e.g. ticking a box or e-mail confirmation) – leaving much of it to interpretation.

Secondly, an area of debate in the RTS is data scraping, which is the practice of third-party providers (Payment Initiation Service Providers and Account Information Service Providers) to access bank accounts on the client's behalf using the client's username and password credentials. This practice was prohibited in the European Banking Authority's final draft RTS.

However, the European Commission urged the EBA not to ban data scraping outright but to hold it in reverse, as a back-up mechanism should bank interfaces (APIs) fail to function properly. It is now for the European Commission to make the final decision on the text of the RTS.

As such, when data scraping is used, it is very difficult, if not impossible for banks to give access only to consented data and simultaneously comply with the other protection requirements related to sensitive data. TPPs can obtain consent for the use of consumer data, or have it covered contractually, but such a bypass is unnecessary if TPPs utilise dedicated interface APIs. Hence, it is unlikely that banks will be able to know if and what consent has been provided by the customers. Under GDPR, banks are fully responsible for the processing performed by third parties, and lack of agreement would not be in compliance with GDPR. Furthermore, banks' responsibility for this kind of processing remains unclear in the absence of any contractual agreement. This practice, then, goes by definition against the spirit of consumer protection and controller liabilities embodied in GDPR and PSD2.

TPPs will likely initiate the process of securing customers' consent, including consent for their activities and the use of the data once obtained. Banks will ultimately remain responsible for confirming the consent directly with their customers. This will probably include confirming details such as the identity of the TPP, what data customers wish to share and how frequently, and when such consent will expire. Such a two-way route – obtaining and confirming consent – has the potential to provide greater protection to TPPs, banks and customers, compared to banks relying solely on the consent provided by the TPPs.

How to navigate through conflicting regulations

Banks and TPPs must create rules and processes for data breaches and build a Data-Safe culture, developing policies regarding better and frequent implementation, training, monitoring and assessment. ➔

Paul Weiss

Management Consulting Analyst

Accenture

Anupam Majumdar

Management Consulting Manager

Accenture

About Paul Weiss and Anupam Majumdar: Anupam Majumdar and Paul Weiss work within Accenture's Consulting Practice, Financial Services, based out of the Netherlands. Both have worked with multi-nationals to define their business and technology strategy and then playing a role executing and delivering against that strategy.

About Accenture: Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital technology and operations. Accenture has extensive experience in payments, Everyday Banking, open APIs and digital banking strategies – and can help organisations navigate the optimal route along this journey.
www.accenture.com

www.accenture.com

Share this story

Secondly, it is important to implement privacy by design, analyse the personal data processing framework in place and review the third-party policies, procedures and contracts.

The technical and operational process for onboarding TPPs will become critical because banks must be prepared to take on an additional financial risk, sharing liability for any breaches. Banks and API providers must start to tackle the privacy problem from the beginning, ensuring that TPPs have sound privacy certification and settings during the onboarding process. Banks and API providers must implement due diligence mechanisms and processes for onboarding TPPs, testing APIs and managing incidents.

Anticipating on (future) TPP requests, privacy design strategies need inclusion. Consent must be a top priority since sharing customer data without proper consent is a clear GDPR violation. Consent is one area where effective identity management is crucial. Identity management is making progress as more secure and user-friendly biometrics replace clunky username and password combinations in order to better verify and authenticate individuals. Banks and TPPs should develop advanced data analytics to prevent more effectively fraud and false identity representations.

Conclusion

Banks hold a monopoly over their customer's data but – under PSD2 – TPPs will now be able to retrieve customer account information and make payments on their behalf. Further guidance is urgently needed from both EU and national regulators on how banks can reconcile the requirements under PSD2 and GDPR.

Organised By

ums CONFERENCES

RISE OF

THE DIGITAL ECONOMY

Cyber Preparedness for New Threat Vectors

2ND ANNUAL

FINSEC

THE BANKING SECURITY SUMMIT

05-06 MARCH, 2018 | DUBAI, UAE

www.newagebankingsummit.com/finsec

Insights on:

Blockchain, Artificial Intelligence and Machine Learning, IoT Security Framework, Ransomware, Frauds and Breaches, Protection against Malware Attacks, Mobile Banking Platforms, Adaptive Authentication, Endpoint Security, Data Analytics, Regulatory Compliance

info@umsconferences.com

Infographic –
Key Players in the Consumer Identity and Access Management Industry

Identity Verification and Online Authentication Solution Providers

CASBs / Platform Providers

GIGYA, janrain, salesforce, ca technologies, okta, loginradius, onelogin, AVATIER, TRANSMIT SECURITY, IBM, Microsoft, Centrify, FORGEROCK, Ping Identity, SECUREAUTH, SailPoint, welcome

Identity Verification / Onboarding

Derived Identification

iSignthis, SIGNICAT, idensys, EPS, iDEAL, iDIN, MyBank, DigiD, Gro, SOFORT, Bancontact

Identity Document Verification

IDnow, hooyu, ENVESTNET YODLEE, KOFAX, id:analytics, DIRECTID, Trulioo, gemalto, onfido, SOCURE, JUMIO, Mitek

Other Means of Verification

BehavioSec, onfido, Trulioo, SOCURE, BIOCATCH, Mitek, JUMIO, Idscan, LexisNexis, ThreatMetrix, NU Data Security, IDnow, MY PINPAD, PROVENIR, PHONIC

Additional checks / compliance

NameScan, Trulioo, fiserv., onfido, id:analytics, DIRECTID, NICE ACTIMIZE, LexisNexis, gemalto, Experian, Idscan, veriphy

Online Authentication

Biometric Authentication (behavioral and physical)

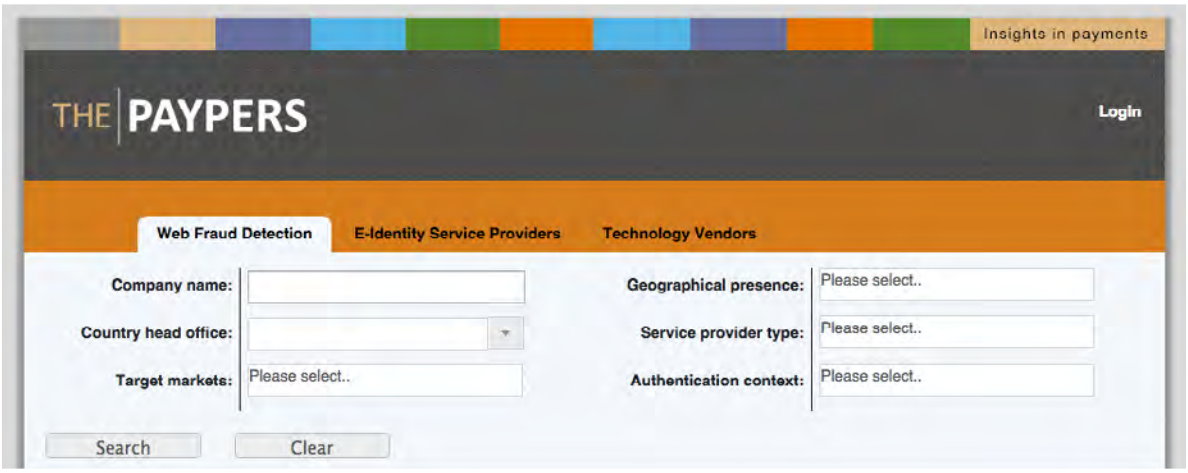
SOCURE, BIO-key, BIOCATCH, bioconnect, BioID, BioSig-ID, ValidSoft, HID, Daon, JUMIO, iovation, feedzai, gemalto, VASCO, CARDINAL COMMERCE, hooyu, IDEMIA, FacePhi, ai, mepin, VERIDIUM, Mitek, MY PINPAD, NICE, NU Data Security, nok nok, pindrop, VerifyMe, Ping Identity, PRECISE, protectoria, SECUREAUTH, SECUREDTOUCH, sift science, zwipe, BehavioSec, simility, ThreatMetrix, Trulioo, EASYSOLUTIONS, UL

Other Authentication Means

Accertify, CyberSource, ethoca, EverCompliant, FEATURE SPACE, G2 Web Services, IDOLOGY, Kount, iSignthis, ai, SIGNICAT, RSA, WEBSHIELD, AU10TIX, RISK IDENT, Entersekt, PHONIC, ACI UNIVERSAL PAYMENTS

THE PAYPERS

Visit Our Enhanced Online Company Profiles Database



All company profiles in the Web Fraud Prevention & Online Authentication Market Guide are available online in an enhanced company profiles database, complete with keywords, company logo and advanced search functionality.

https://webfraud-eidentity.thepaypers.com/

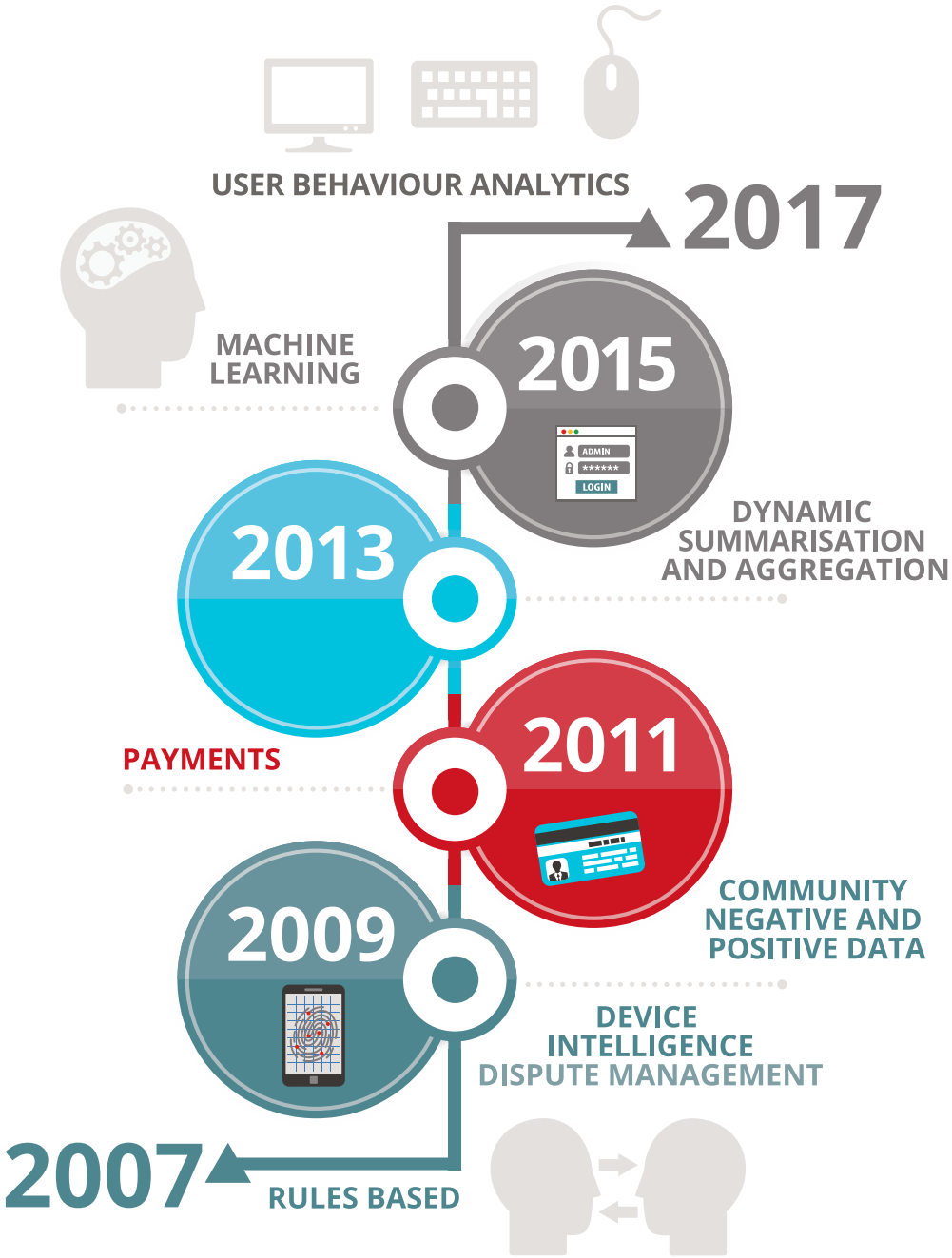
Company Profiles

Company	Accertify, Inc. View company profile in online database
	Accertify, Inc., a wholly owned subsidiary of American Express, is a leading provider of fraud prevention, disputes management, and payment gateway solutions to merchant customers spanning diverse industries worldwide. Accertify's suite of products and services help ecommerce companies grow their business by driving down the total cost of fraud and protecting their brand.
Website	www.accertify.com
Keywords for online profile	fraud, disputes management, payment gateway, risk, protect, loss, Accertify
Business model	Software-as-a-service (SaaS)
Target market	Retail, travel, ticketing and entertainment, financial institutions, payment service providers, government services, marketplaces, gaming and gambling, other ecommerce
Contact	emea@accertify.com
Geographical presence	Global
Active since	2007
Service provider type	Digital identity service provider, technology vendor, web fraud detection company, payment service provider (PSP)
Member of industry association and or initiatives	Merchant Risk Council (MRC), AMIPCI
Services	
Unique selling points	Accertify leverages its flexible platform to enable merchants to screen for multiple fraud use cases, including, but not limited to payment, loyalty, claims, staff and social media reputation. Our unique capabilities allow genuine customers to be efficiently removed from fraud processes, supporting merchant growth.
Core services	Accertify's core suite of services includes fraud management, disputes management, and payment gateway.
Pricing Model	For more details contact our sales team at emea@accertify.com
Fraud prevention partners	Accertify is integrated to multiple third party services which includes, but not limited to: InAuth, Emailage, LexisNexis, ethoca, Whitepages, Mastercard, eBureau and NU Data Security.
Other services	Professional services, decision sciences, manual review outsourcing 24/7, support services, rule management and improvement, best practice consulting, training services
Third party connection	United Parcel Services (UPS) and FedEx to obtain proof of delivery signatures; eFax (inbound and outbound fax receipt); global distribution systems (Amadeus, Navitaire, Sabre).
Technology: anti-fraud detection tools available	
Address verifications services	Yes
CNP transactions	Yes
Card Verification Value (CVV)	Yes
Bin lookup	Yes
Geo-location Checks	Yes
Device Fingerprint	Yes, through integrated partners
Payer Authentication	Yes
Velocity Rules – Purchase Limit Rules	Yes
White list/black list database	Yes
KYC – Know Your Customer	Yes; complemented with integrated partners
Credit Rating	No
Follow up action	Additional authentication (out-of-band authentication) and transaction verification capabilities
Other	Profiling (dynamic summarisation and aggregation)

Authentication Context	
Online	Yes
Mobile	Yes
ATM	No
POS	Yes
Call centre	Yes
Other	Kiosk (unattended terminal)
Reference Data connectivity	
Connectivity to governmental data	Yes, provided via partner – for example Experian or Lexis Nexis
Other databases	BIN, Oanda, Global latitude/longitude, Accertify Risk ID (multi-merchant negative dB), Accertify Index (multi-merchant positive dB), Amex Risk Information Management dB
Fraud management system type	
Single-channel fraud prevention system	Yes
Multi-channel fraud prevention system	Yes
Certification	
Type	PCIDSS Level 1, ISO 27001
Regulation	For more details contact our sales team at emea@accertify.com
Other quality programms	For more details contact our sales team at emea@accertify.com
Other remarks	
Clients	
Main clients / references	Please reference our website at: http://www.accertify.com/en/resources/#CaseStudies
Future developments	For more details contact our sales team at emea@accertify.com

As fraud evolves, so do we

Proven hosted software solutions and knowledgeable, expert services to safeguard each step of the payment lifecycle.



accertify.com

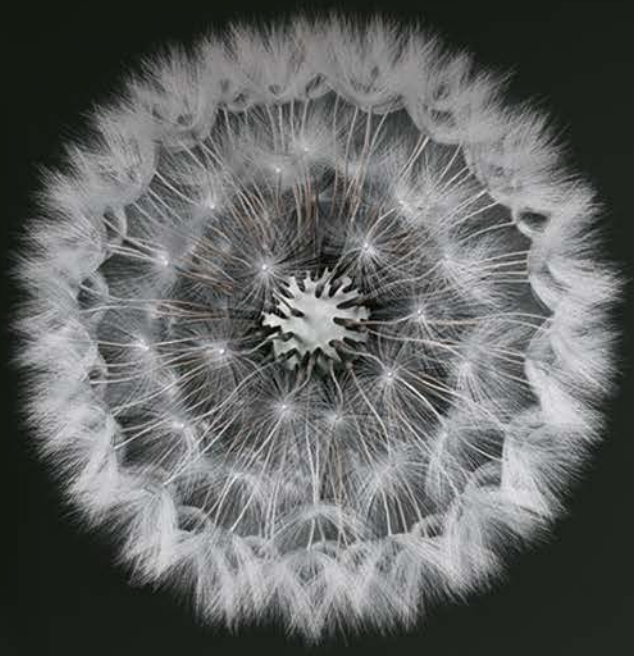
Accertify
AN AMERICAN EXPRESS COMPANY

1st Floor Belgrave House, 76 Buckingham Palace Rd, London SW1W 9AX, UK.

Company	ACI Worldwide	View company profile in online database
	A leading global provider of real-time electronic payment and fraud solutions, offering fraud prevention for all payment transaction types to merchants, banks and processors. Through ACI ReD Shield, we deliver real-time, multi-tiered fraud solutions which are managed by expert risk analysts. Our service is informed by our unrivalled access to data, our strong business intelligence capabilities and ability to connect merchants, acquirers and issuers in the fight against fraud.	
Website	www.aciworldwide.com	
Keywords for online profile	online fraud prevention, ecommerce, online fraud, fraud analytics	
Business model	Direct to merchants and indirectly, through reseller partners	
Target market	Online ecommerce merchants, financial institutions, payment services providers, government services, acquirers, gaming, retail, hospitality, loyalty, telecommunications, travel and entertainment	
Contact	Andy McDonald (andy.mcdonald@aciworldwide.com or +44 (0)7785 627494)	
Geographical presence	Global	
Active since	1975	
Service provider type	Digital identity service provider, technology vendor, web fraud detection company, payment service provider (PSP), issuer, acquirer	
Member of industry association and or initiatives	Merchant Risk Council, IMRG, Vendorcom	
Services		
Unique selling points	Automated processes and dedicated support from expert risk analysts; global fraud data, fraud solutions tailored to sector and customer needs, predictive models and unlimited, flexible rules; holistic fraud management – real-time and post-transaction monitoring using our unrivalled business intelligence solution; presence across the payments chain, supporting merchant and issuer collaboration in the fight against fraud.	
Core services	Card Not Present (online, IVR, call centre and mobile) and card present fraud prevention, fraud and risk consultancy, payment services	
Pricing Model	Flexible	
Fraud prevention partners	ACI partners with leading PSPs around the globe (see a full list at http://www.aciworldwide.com/who-we-are/partners/our-partners.aspx).	
Other services	Payment services: Base 24- EPS, Postilion, ACI Proactive Risk Manager, ACI Universal Online Banker. Please visit www.aciworldwide.com to view all services available from ACI.	
Third party connection		
Technology: anti-fraud detection tools available		
Address verifications services	Yes	
CNP transactions	Yes	
Card Verification Value (CVV)	Yes	
Bin lookup	Yes	
Geo-location Checks	Yes	
Device Fingerprint	Yes	
Payer Authentication	Yes	
Velocity Rules – Purchase Limit Rules	Yes, unlimited and flexible.	
White list/black list database	Yes	
KYC – Know Your Customer	Yes	
Credit Rating	No	
Follow up action	Yes	
Other	Compliance list checking, AML, additional black lists	

Authentication Context	
Online	Yes
Mobile	Yes
ATM	Yes
POS	Yes
Call centre	Yes
Other	For more information, please contact the sales team.
Reference Data connectivity	
Connectivity to governmental data	
Other databases	Commercial attribute providers, e.g. credit databases
Fraud management system type	
Single-channel fraud prevention system	Yes
Multi-channel fraud prevention system	Yes
Certification	
Type	PCI DSS v3.0, ISO 27001, ISO 9001, SAS70 (e.g. ISO 27001, ISO 9001, TS 101 456, SAS70)
Regulation	EU Data Protection (KYC)
Other quality programms	UK Payments Administration accreditation, Visa Account Information Security (AIS and CISP) accreditation, Amex Data Security Operating Policy (e.g. ethical hacking, privacy compliance)
Other remarks	For more information, please contact the sales team.
Clients	
Main clients / references	More information available upon request.
Future developments	For more information, please contact the sales team.

ACI UNIVERSAL PAYMENTS℠



TURN SUSCEPTIBLE INTO SECURE.

Protect your online payments while driving business growth.
aciworldwide.com/onlinefraudprevention

Company	BioCatch	View company profile in online database
	BioCatch is a cybersecurity company that delivers behavioral biometrics, analysing human-device interactions to protect users and data. Banks, financial institutions and other enterprises use BioCatch to significantly reduce online fraud and friction costs, and protect against a variety of cyber threats, without compromising the user experience.	
Website	https://www.biocatch.com/	
Keywords for online profile	Behavioral biometrics, identity proofing, continuous authentication, fraud prevention	
Business model	BioCatch leverages behavioral biometrics to track user interactions and responses within web and mobile applications. This provides banks, ecommerce companies and other enterprises with a strong value proposition: we can detect the most advanced fraud attacks and cyber threats with an amazing degree of accuracy. We provide business value in two primary areas: Less Friction. BioCatch Behavioral Biometrics authenticates over a very high percentage of genuine sessions thus reducing the number of failed authentication attempts and associated operational call center costs. Less Fraud: BioCatch is able to prevent various types of fraud, such as social engineering schemes and non-human attacks by bots, aggregators, malware and remote access Trojans.	
Target market	banking, ecommerce, financial services (e.g, credit bureaus and unions), credit card issuers, insurance, payroll systems and mobile device manufacturers.	
Contact	Kevin Donovan, VP of Sales, Americas, kevin.donovan@biocatch.com; Richard Perry, VP of Sales, EMEA, richard.perry@biocatch.com	
Geographical presence	BioCatch has a strong global presence in all geographic territories. In particular, the US, EMEA and LATAM.	
Active since	2011	
Service provider type	BioCatch is a technology vendor that is capable of identifying sophisticated forms of account takeover through behavioral profiling and threat detection without impacting the user experience. This is used to either escalate a session or activity that receives a high score, or alternatively to de-escalate the activity even if other security or fraud controls suggest it is risky, allowing the customer to reduce friction and operational costs. BioCatch excels in providing a near-Zero-FP detection of a variety of advanced attacks: bots, MITB attack, social engineering and RATs (Remote Access).	
Member of industry association and or initiatives	American Banking Association, Biometrics Institute.	
Services		
Unique selling points	Technology: BioCatch's unparalleled patent portfolio drives extremely high accuracy with minimal false alarms; Experience: BioCatch's solution is widely deployed by leading banks and financial institutions around the world; Expertise: BioCatch is spearheaded by a strong "bench" of experts from various scientific disciplines.	
Core services	BioCatch behavioral biometrics has three primary capabilities that provide great value to customers: Identity Proofing, Continuous Authentication (through passive behavioral profiling) and Fraud Prevention. In regards of fraud prevention, BioCatch is able to effectively combat a variety of threats, such as: malware, bots/aggregators, remote access Trojans and social engineering.	
Pricing Model	BioCatch's pricing model is based on an annual license and a one-time setup fee per user or transaction basis.	
Fraud prevention partners	BioCatch has partnerships with: Microsoft, LexisNexis, Nuance, Experian, Samsung SDS.	
Other services	For Identity Proofing BioCatch behavioral biometrics offers a new dimension to fighting new account fraud. The system distinguishes between a real user and an impostor by recognising normal user behavior and fraudster behaviors, even when no profile exists. Understanding how criminals behave online, the BioCatch Identity Proofing Module looks at 3 elements to generate a risk score: **Application Fluency**: Most fraudsters use compromised or synthetic identities to repeatedly attack a site. These actions show a fluency with the site and the process used to open a new account; **Navigational Fluency**: Fraudsters often use advanced computer skills that are rarely seen among real users. Common examples include keyboard shortcuts and function keys; **Low Data Familiarity**: Fraudsters exhibit several behavioral traits when they enter in unfamiliar data.	

Third party connection	BioCatch has numerous business partnerships, for example with Experian, a leading a consumer credit reporting agency that collects and aggregates information on over one billion people and businesses; Nexis, which provides computer-assisted legal research, as well as business research and risk management services. BioCatch has a very strong and ever-growing partnership with Microsoft: BioCatch technical operations are supprted by Microsoft Azure.
Technology: anti-fraud detection tools available	
Address verifications services	N/A
CNP transactions	N/A
Card Verification Value (CVV)	N/A
Bin lookup	N/A
Geo-location Checks	Yes
Device Fingerprint	Yes
Payer Authentication	Yes
Velocity Rules – Purchase Limit Rules	N/A
White list/black list database	Yes
KYC – Know Your Customer	Yes
Credit Rating	N/A
Follow up action	BioCatch's technology is built to support risk-based authentication, by feeding profiling scores into ther platform rules engines. The platforms usually specify the follow-up actions on a case by case basis.
Other	Invisible Challenges are patented techniques that introduce subtle tests into the online session that users subconsciously respond to without sensing any change in their experience. The response contains behavioral data that is used to distinguish a real user from an imposter, whether human or non-human (robotic activity, malware, aggregator, etc.). It is important to note that BioCatch's team of researchers test each challenge and its corresponding deviation to determine the threshold at which users notice a change in experience on the mobile or website.
Authentication Context	
Online	Yes. We support JavaScript integrations with the following browsers: Internet Explorer, Chrome, Firefox.
Mobile	Yes. We support SDK integrations with iOS and Android.
ATM	N/A
POS	N/A
Call centre	N/A
Other	N/A
Reference Data connectivity	
Connectivity to governmental data	N/A
Other databases	N/A
Fraud management system type	
Single-channel fraud prevention system	Yes
Multi-channel fraud prevention system	Cross-Channel Fraud: Many customers use BioCatch to detect fraud that begins or ends in the online channel, but then is carried out in a different channel. The combination of abnormal behaviour with a risky context is a highly accurate method, with minimal false positives.

Certification	
Type	SOC 2 Type II: BioCatch complies with highest security standards when it comes to security. BioCatch is SOC2 Type II[1] (Security and Availability) certified since February 15th 2015 by E&Y.
Regulation	BioCatch complies with GDPR, PSD2 and Open Banking Initiatives.
Other quality programms	
Other remarks	
Clients	
Main clients / references	BioCatch is implemented in global tier-1 financial institutions, with +5 billion transaction per month covering more than +50 million users. Detailed Case studies at: http://www.biocatch.com/resources/case-studies/download-leading-uk-bank-adds-high-risk-mobile-functionalities-with-behavioural-authentication http://www.biocatch.com/resources/case-studies/download-top-5-uk-retail-bank-detects-account-takeover-with-behavioural-biometrics http://www.biocatch.com/resources/case-studies/download-top-5-uk-bank-detects-remote-access-trojans Individual reference details for each bank available on request.
Future developments	In 2018, BioCatch is planning on massive expansion of use cases, as the capability of behavioral biometrics extends beyond the traditional fraud prevention realm into on-device authentication and new fraud areas, and new verticals, to go beyond banking and expanded partnerhips.

Company	buguroo	View company profile in online database
	Cybersecurity company founded in 2010. buguroo is specialised in the development of software for online fraud prevention. bugFraud detects cyberthreat thanks to the development of next generation technologies based on deep learning (artificial intelligence), neural networks and behavioral analysis biometrics.	
Website	www.buguroo.com	
Keywords for online profile	fraud, online fraud prevention, behavioral biometric, artificial intelligence, deep learning, online banking, deep neural networks, cybersecurity	
Business model	Subscription and licence	
Target market	Financial institutions, payment services providers	
Contact	sales@buguroo.com	
Geographical presence	LATAM, US, EUROPE	
Active since	2010	
Service provider type	Web fraud detection company	
Member of industry association and or initiatives	N/A	
Services		
Unique selling points	- Unique web content shield approach for detecting phishing and malware attacks; - Deep learning for continuous online user's cognitive analytics and behavioral biometry monitoring for detecting ATO and RAT threats; - Holistic technological view of online user's session correlating data from web content, biometry, omnichannel protection, device fingerprint, access network and threat Ingelligence; - 100% users protected with Frictionless approach.	
Core services (max 20 words)	Online fraud prevention	
Pricing Model	Based on online users protected	
Fraud prevention partners	Deloitte, Multisoft, G&D, Netsafe, Lidera and others	
Other services	Account Takeover (ATO), Remote Acces Trojan (RAT), advanced forensic and Reversing Malware services, intelligence and e-crime services, integration services with third party fraud solutions: SIEM, transaction monitoring,etc.	
Third party connection	SIEM	
Technology: anti-fraud detection tools available		
Address verifications services	N/A	
CNP transactions	N/A	
Card Verification Value (CVV)	N/A	
Bin lookup	N/A	
Geo-location Checks	N/A	
Device Fingerprint	N/A	
Payer Authentication	N/A	
Velocity Rules – Purchase Limit Rules	N/A	
White list/black list database	N/A	
KYC – Know Your Customer	N/A	
Credit Rating	N/A	
Follow up action	N/A	
Other	behavioral biometrics and deep learning (neural network)	

Authentication Context	
Online	Yes
Mobile	Yes
ATM	N/A
POS	N/A
Call centre	N/A
Other	N/A
Reference Data connectivity	
Connectivity to governmental data	N/A
Other databases	N/A
Fraud management system type	
Single-channel fraud prevention system	N/A
Multi-channel fraud prevention system	N/A
Certification	
Type	N/A
Regulation	N/A
Other quality programms	N/A
Other remarks	Cool Vendor 2016 by Vendor; “Overall Fraud Prevention Solution of the Year 2017” Cybersecurity BreakTrought Award; Most promising Cybersecurity solution in 2017” by CIO review Magazine.
Clients	
Main clients / references	online banking – More information available upon request
Future developments	More information available upon request

®bugFraud

COMBACT FRAUD WITH CUTTING EDGE TECHNOLOGIES

®buguroo

DEEP LEARNING FOR ONLINE FRAUD PREVENTION

Calle Anabel Segura, 16 Edificio 3 Planta 1 · Alcobendas · 28108 · Madrid · Spain
www.buguroo.com · info@buguroo.com · (+34) 91 229 43 49

Company	CyberSource Ltd. View company profile in online database
CyberSource® the power of payment	CyberSource, a wholly owned subsidiary of Visa, Inc., is the only integrated payment management platform built on secure Visa infrastructure, with the payment reach and fraud insights of a massive USD 358 billion global processing network. CyberSource and Authorize.Net payment management solutions help 465,000 large and small businesses worldwide grow sales, mitigate risk, and operate with greater agility. For more information, please visit www.cybersource.co.uk
Website	www.cybersource.co.uk
Keywords for online profile	fraud management, risk management, payment security, ecommerce, payments, payment gateway, account takeover, rules-based payer authentication, loyalty fraud
Business model	Software as a Service (SaaS)
Target market	Retail, travel, financial institutions, media and entertainment
Contact	CyberSource Ltd, Kennet Wharf, 41-45 Queens Road, Reading, RG1 4BQ
Geographical presence	Worldwide
Active since	1994
Service provider type	Payment Service Provider (PSP), fraud management company, web fraud detection, device identification
Member of industry association and or initiatives	Merchant Risk Council, IMRG, Vendorcom
Services	
Unique selling points	The only global payment management platform built on secure Visa infrastructure—with integrations to the world's largest network of connected commerce partners and transaction insights—CyberSource solutions power businesses to create new brand experiences, grow sales and engagement, and keep payment operations safe.
Core services	The CyberSource fraud management platform offers a complete range of comprehensive, holistic fraud management solutions to help identify and mitigate fraud quickly, accurately, and with little manual intervention – from account monitoring to transaction fraud detection, rules tuning to payer authentication.
Pricing Model	Tiered SaaS-based pricing model
Fraud prevention partners	ThreatMetrix, Cardinal Commerce, Neustar
Other services	More information available upon request
Third party connection	Neustar, LexisNexis, Whitepages.com, Perseuss, Computer Services, Emailage
Technology: anti-fraud detection tools available	
Address verifications services	Yes
CNP transactions	Yes
Card Verification Value (CVV)	Yes
Bin lookup	Yes
Geo-location Checks	Yes
Device Fingerprint	Yes
Payer Authentication	Yes
Velocity Rules – Purchase Limit Rules	Yes
White list/black list database	Yes
KYC – Know Your Customer	No
Credit Rating	No
Follow up action	Additional authentication (out of band authentication) and transaction verification capabilities
Other	More information available upon request

Authentication Context	
Online	Yes
Mobile	Yes
ATM	No
POS	No
Call centre	Yes
Other	More information available upon request
Reference Data connectivity	
Connectivity to governmental data	No
Other databases	Commercial attribute providers, e.g. credit databases
Fraud management system type	
Single-channel fraud prevention system	No
Multi-channel fraud prevention system	Yes
Certification	
Type	More information available upon request
Regulation	More information available upon request
Other quality programms	More information available upon request
Other remarks	Contact europe@cybersource.com for more information
Clients	
Main clients / references	GAME, GHD, Aeromexico, Turkish Airlines, Cinépolis, Webjet, Backcountry, ESET
Future developments	For more information contact europe@cybersource.com

CyberSource®

No single machine learning model can spot every fraud. That's why we married three together.

CyberSource Decision Manager doesn't just use one approach to tackle fraud. It blends the best of self-learning and static machine learning, plus insights from the world's largest fraud detection radar. Then it adds a flexible rules engine you can tweak when a new threat starts to appear. So you're set to prevent fraud, any time, anywhere.

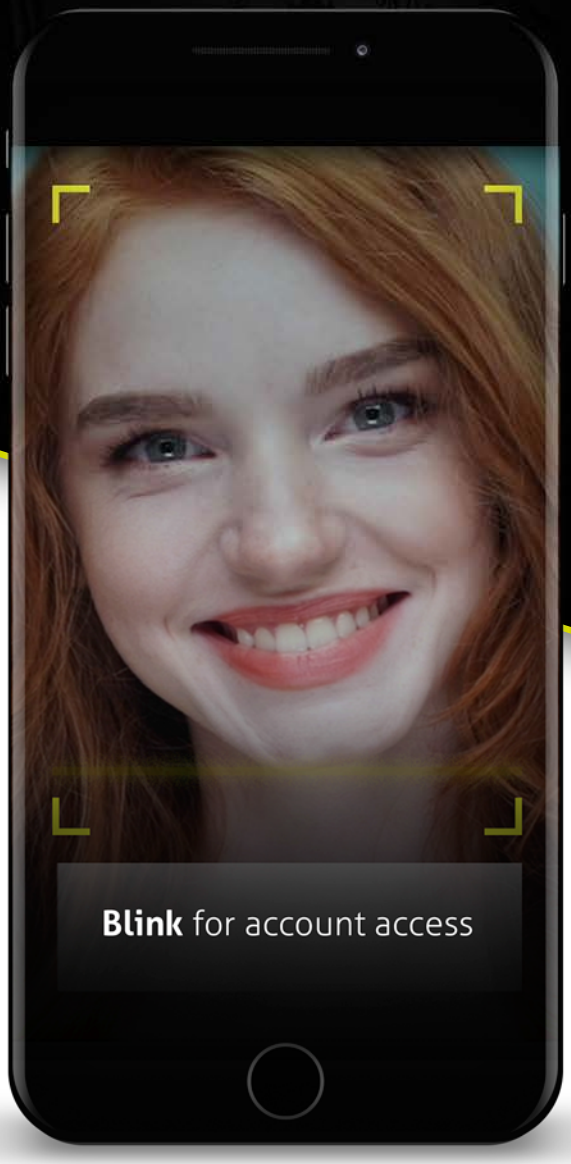
www.cybersource.co.uk

Company	Easy Solutions	View company profile in online database
EASYSOLUTIONS A CYXTERA BUSINESS	Easy Solutions is a security provider focused on the comprehensive detection and prevention of electronic fraud across all devices, channels and clouds. Products range from digital threat protection and secure browsing to multi-factor authentication and transaction anomaly detection, offering a one-stop shop for end-to-end fraud protection.	
Website	www.easysol.net	
Keywords for online profile	electronic fraud prevention, detection, authentication, behavioral analytics, anti-phishing	
Business model	Software as a Service (SaaS) and On-Premise	
Target market	Financial Institutions, enterprises	
Contact	sales@easysol.net	
Geographical presence	Global	
Active since	2007	
Service provider type	Anti-fraud security vendor	
Member of industry association and or initiatives	American Bankers Association, FIDO, Anti-Phishing Working Group, Global Cyber Alliance	
Services		
Unique selling points	Total Fraud Protection gives Easy Solutions an advantage at proactive take-down, monitoring, identification and interception, effectively mitigating fraud before it happens. This approach reduces false positives and the overhead of managing tools while lowering the costs associated with supporting an anti-fraud program.	
Core services (max 20 words)	Digital treat protection, end-point protection, authentication, behavioral analytics, email authentication, biometrics	
Pricing Model	Subscription-based	
Fraud prevention partners	Q2 eBanking	
Other services	Account takeover, new account registration, payment fraud prevention, frictionless authentication, bot detection, professional services, malware detection	
Third party connection	Fraud analytics for customers, international address verification	
Technology: anti-fraud detection tools available		
Address verifications services	No	
CNP transactions	No	
Card Verification Value (CVV)	No	
Bin lookup	No	
Geo-location Checks	No	
Device Fingerprint	Yes	
Payer Authentication	Yes	
Velocity Rules – Purchase Limit Rules	Yes	
White list/black list database	No	
KYC – Know Your Customer	No	
Credit Rating	No	
Follow up action	Out of band authentication, takedown	
Other	Profiling (dynamic summarisation and aggregation)	
Authentication Context		
Online	Yes	
Mobile	Yes	
ATM	Yes	
POS	Yes	
Call centre	Yes	
Other	Yes	

Reference Data connectivity	
Connectivity to governmental data	No
Other databases	No
Fraud management system type	
Single-channel fraud prevention system	Yes
Multi-channel fraud prevention system	Yes
Certification	
Type	SSAE 16 Type 1 SOC 2
Regulation	
Other quality programms	
Other remarks	Deloitte Technology Fast500, Strong Performer on Forrester Wave: Risk Authentication, Cited in Gartner Market Guide for Online Fraud Fetection.
Clients	
Main clients / references	
Future developments	

ORGANIZATIONS LOSE $7 BILLION

DUE TO ACCOUNT TAKEOVER EACH YEAR*



Strike the right balance between security and convenience with

BIOMETRIC AUTHENTICATION

Move beyond passwords and tokens. Take advantage of innovative biometric technology that leverages user fingerprints, voices and facial features to enable simple and secure access.

Combine biometrics with one or more factors for the easiest and safest authentication method available today.

sales@easysol.net

EASYSOLUTIONS®
A CYXTERA BUSINESS

w w w . e a s y s o l . n e t

*Forrester

Company	Emailage	View company profile in online database
emailage® The Global Hub of Email Intelligence	Founded in 2012 and with offices in Phoenix, London and Sao Paulo, Emailage is a leader in helping companies significantly reduce online fraud. Through key partnerships, proprietary data, and machine-learning technology, Emailage builds a multi-dimensional profile associated with a customer's email address and renders a predictive risk score.	
Website	www.emailage.com	
Keywords for online profile	online fraud prevention, email risk assessment, email address fraud prevention, CNP fraud prevention	
Business model		
Target market	Online ecommerce merchants, financial institutions, airlines, OTA, ticketing brockers, money transfer companies, credit card issuers, marketplace lenders, personal computer manufacturers, fraud platforms, gaming and gambling, other online businesses	
Contact	Contact@emailage.com	
Geographical presence	Global	
Active since	2012	
Service provider type	Web fraud detection company	
Member of industry association and or initiatives	Merchant Risk Council	
Services		
Unique selling points	Emailage's Software-as-a-Service solution delivers powerful, real-time risk intelligence by leveraging the email address as a unique global identifier. Emailage combines vast email transaction history, machine learning algorithms and positive and negative data to generate a predictive risk score, which helps improve the risk assessment of any transaction where an email address is provided. Use cases include online transactions, new accounts/sign up process, customer account maintenance, and marketplace listings.	
Core services	Email address + Global network + machine learning algorithms = online predictive fraud risk score. We provide a secure, frictionless layer of protection that will supercharge your risk engine. Our predictive online fraud risk scoring uses email address metadata as the core for transactional risk assessment and identity validation. Our online identity profiles fuse this data with other elements, such as phone number, address and customer name. Emailage helps reduce fraud for hundreds of customers around the world, including 5 of the top 10 global retailers, 3 of the top 5 largest global airlines, the top 3 PC manufacturers, 3 of top 6 credit card issuers, 3 of the top 5 marketplace lenders, the top 4 money transfer providers, and 3 of the top 5 travel websites. This year to date, Emailage has analysed nearly USD 100 billion in transaction volume and identified over 17 million high-risk transactions.	
Pricing Model	SaaS	
Fraud prevention partners	Accertify, CyberSourse, Experian, Equifax, Kount	
Other services	N/A	
Third party connection	Accertify, CyberSourse, Experian, Equifax, Kount	
Technology: anti-fraud detection tools available		
Address verifications services	Along with the email address, the billing and shipping addresses can also be passed to Emailage for a hoslistic risk assessment, which will help increase the fraud coverage with a higher fraud hit rate.	
CNP transactions	Yes, the Emailage Email Risk Assessment solution was design to be used as a up-front fraud decision for Card Not Present transactions for every online transaction where the email address is provided.	
Card Verification Value (CVV)	N/A	
Bin lookup	Yes, starting 1Q2018	
Geo-location Checks	Yes, for the online transactions, Emailage also receives the IP Address of the transaction, which is used for geo location risk assessment, along with the billing and shipping address.	
Device Fingerprint	N/A	
Payer Authentication	N/A	

Velocity Rules – Purchase Limit Rules	Yes, Emailage provides velocity controls.
White list/black list database	Emailage has the biggest global database of fraudulent emails, with more than 50 million records and growing by 1M a month; this data is directly used on our risk decision engine and modules to identify fraud trends, patterns and behaviours.
KYC – Know Your Customer	N/A
Credit Rating	N/A
Follow up action	Additional authentication (out of band authentication) and transaction verification capabilities
Other	Emailage provides merchants with the ability to verify the digital identity of the consumers for every transaction, making it hader for fraudsters to penetrate. So, instead the basic transaction risk assessment, the Emailage Email Risk Assessment can verify who is behind each online transaction, providing a holist risk assessment and adding stronger controls against fraudsters while helping approving the good customers. This approach can prevent mass attacks and reduce the ability of fraudsters to scale.
Authentication Context	
Online	Yes, the Emailage Email Risk Assessment solution was design to be used as a up-front fraud decision online transactions, it can add value every time an email address is provided on a transaction.
Mobile	N/A
ATM	N/A
POS	N/A
Call centre	N/A
Other	N/A
Reference Data connectivity	
Connectivity to governmental data	N/A
Other databases	Social media data, IP address geolocation and proxy information, domain attributes and phone ownership and carrier data.
Fraud management system type	
Single-channel fraud prevention system	No
Multi-channel fraud prevention system	Yes
Certification	
Type	SOC (Service Organisation Controls), The EU-U.S. and Swiss-U.S. Privacy Shield Framework
Regulation	N/A
Other quality programms	N/A
Other remarks	Add other certifications
Clients	
Main clients / references	5 of the top 10 global retailers, 3 of the top 5 largest global airlines, the top 3 PC manufacturers, 3 of top 6 credit card issuers, 3 of the top 5 marketplace lenders, the top 4 money transfer providers, and 3 of the top 5 travel websites
Future developments	Online digitial identify, rapid risk assessment, mobile risk attributes, hollistic scoring, rapid risk assessment, digital identity verification, address demographics, address risk assessment, mobile risk indicators, credit card BIN intellegence, enhanced handle pattern detection, portal 3.0, risk profiling real-time, Single Sign On (SSO), replay simulation channel, data normalisation 2.0

emailage®
The Global Hub of Email Intelligence

Strength in numbers: Get the power of shared fraud intelligence

Today's organized fraud rings have no regard for industry or region. The only way to fight back is with the power of a combined network.

Emailage's global intelligence network unites industry leading companies across the globe. **We feature intelligence on over 5 billion unique email address**, with nearly a million more added each month.

Our predictive online fraud risk score uses email address metadata, along with other data elements, as a basis for transactional risk assessment and identity validation.

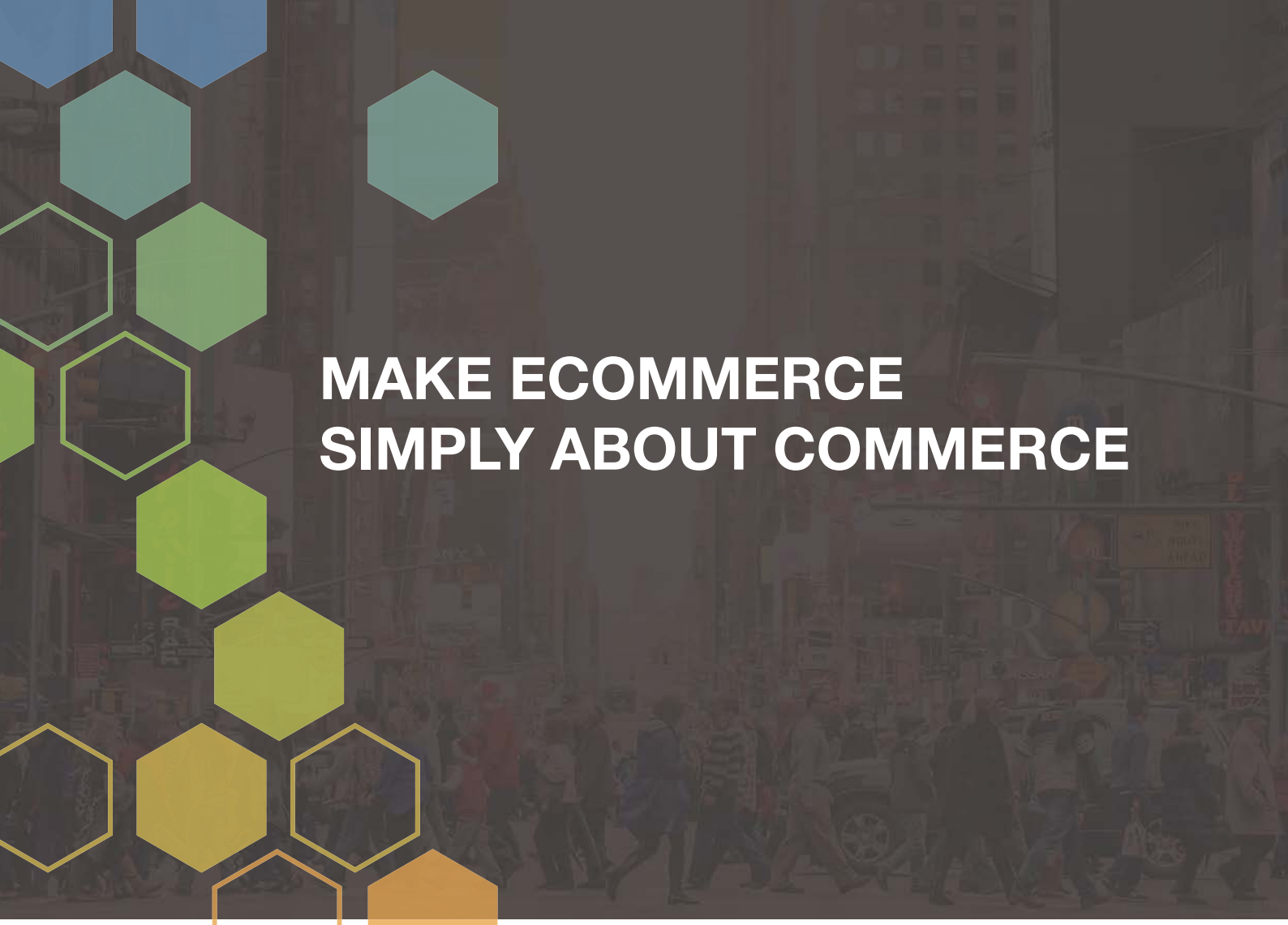
With a clear picture of who is behind a transaction, our customers expedite approvals, prevent chargebacks, automate workflows and optimize manual review.

Company	Entersekt	View company profile in online database
	Entersekt is an innovator in mobile app security and transaction authentication, securing digital banking and payments by harnessing the power of electronic certificate technology with the convenience of mobile phones. Financial institutions look to Entersekt to strengthen the bonds of trust they share with their customers and to deepen those relationships through innovative new services.	
Website	www.entersekt.com	
Keywords for online profile	Mobile app security, mobile banking, online banking, card-not-present, out-of-band authentication, multi-factor authentication, push-based authentication, 3-D Secure, payments enablement, biometrics enablement, transaction signing, phone-as-a-token, regulatory compliance	
Business model	Direct and through partners	
Target market	Financial institutions, card issuers, insurers, payment service providers	
Contact	Entersekt sales team: sales@entersekt.com	
Geographical presence	Africa, Europe, Middle East, North America	
Active since	2008	
Service provider type	Digital identity service provider	
Member of industry associations and intiatives	FIDO Alliance, WASPA	
Services		
Core services	Mobile-app–based, multi-factor authentication and transaction signing of online banking, mobile banking, and card-not-present payments, secure biometrics enablement	
Other services	Non-app-based out-of-band authentication through push USSD, mobile payments enablement	
Unique selling points	Entersekt's patented emCert technology generates public/private key pairs to uniquely identify enrolled mobile devices and validate two-way communications. A self-contained cryptographic stack and communications layer enables an end-to-end encrypted channel, distinct from that initiated by the device, so transactions originating from the phone can still be authenticated out of band on the same device. Highly mature and scalable, the technology is used by tens of millions of end-users globally.	
Pricing model	Per user subscription	
Partners	ABCorp, Amazon Web Services, Backbase, Blue Bay Technologies, CREALOGIX, FIS, Global Kinetic, IBM, IST Networks, Netcetera	
Offering: authentication technology used		
Technology used	Industry-standard X.509 digital certificates, proprietary validation techniques developed specifically for the mobile phone; FIPS 140-2 Level 3 on-premise hardware appliance; dynamic public key pinning, secure browser pattern; device and application context for context-based risk scoring; advanced detection of rooting, jailbreaking, or similar mobile operating system security bypass hacks, secure enablement of fingerprint, voice, iris biometrics; SIM-swap protection; NI USSD for non-app-based out-of-band authentication	
Authentication context		
Online	Yes	
Mobile	Yes	
ATM	No	
Branch/Point of Sale	No	
Call Centre	Yes	
Other	Card-not-present payments (3-D Secure), email, staff portal, access to healthcare and insurance records, PSD2 and GDPR mandates and authorisations	

Issuing process (if applicable)	
Assurance levels conformity	N/A
Online issuing process (incl lead time in working days)	Yes. Identity proofing and enrolment processes are set by the implementing institution, but there is no reason why remote device registration should take more than a few minutes. Options available for enroling a user include phone-based registration via one-time password, scanning a printed QR code, and a combination of scanning a bank card and inputting the associated PIN.
Face-to-face issuing (incl lead time in working days)	Yes. Identity proofing and enrolment processes are set by the implementing institution, but there is no reason why in-branch device registration should take more than a few minutes.
Issuing network	Bank branches, online services
Attributes offered	
Persons Companies	Level of trust (e.g. biometric data, password or PIN, device context, geolocation and more), unique mobile device ID, digitally signed authentication message
Reference data connectivity	
Connectivity to governmental data	N/A
Other databases	N/A
Certification	
Type	Entersekt's flagship product, Transakt, is FIDO Certified as a U2F (universal second factor) authenticator. Transakt is also validated with the Ready for IBM Security Intelligence program. Entersekt's card-not-present authentication solution is fully accredited by Visa, Mastercard, and American Express.
Regulation	Entersekt's solutions are engineered specifically for the heavily regulated financial sector and adhere to all major digital banking security mandates, including the requirements set out by the European Central Bank, the FFIEC, and the Monetary Authority of Singapore. They are compliant with ISO 21188:2006 (public key infrastructure for financial services) and utilise hardware security modules certified as FIPS 140-2 Security Level 3 for encrypting and decrypting all authentication data.
Other quality programs	The underlying technology is regularly validated by independent third parties to ensure it is invulnerable to new attack vectors.
Other remarks	
Clients	
Main clients / references	Those listed in the public domain: Absa, Bayern Card-Services, Capitec Bank, Coutts, Equity Bank, FirstBank of Colorado, Investec, Nedbank, Old Mutual, Pluscard, Swisscard. For others, please contact our sales team.
Future developments	For more information, please contact our sales team.

Company	Ethoca	View company profile in online database
ethoca™	Leveraging a growing, global network of hundreds of card issuers and thousands of ecommerce merchants, Ethoca is the leading provider of collaboration-based technology. Their innovative solutions enable both issuers and merchants to increase card acceptance, stop fraud, recover lost revenue and eliminate chargebacks from fraud and customer service disputes.	
Website	www.ethoca.com	
Keywords for online profile	collaboration, fraud, chargeback, card-not-present, customer disputes, protect, loss, ecommerce	
Business model	Privately held. Sell direct and through partners.	
Target market	Online shoppers, financial institutions, payment services providers, government services, online communities/web merchants, gaming and gambling, other online businesses	
Contact	sales@ethoca.com	
Geographical presence	Global (with offices in Toronto, Austin, London, Paris, Melbourne)	
Active since	2005	
Service provider type	Digital identity service provider, technology vendor, web fraud detection company, payment service provider (PSP), issuer, acquirer	
Member of industry association and or initiatives		
Services		
Unique selling points	Because Ethoca's fraud and dispute intelligence has been confirmed by cardholders with their bank, there is no guesswork. Merchants take immediate action to stop fraudulent orders and refund customers to eliminate chargebacks. Card issuers recover losses on 3D Secure and low value transactions, while avoiding the costly chargeback process altogether.	
Core services	Ethoca Alerts	
Pricing Model	More information available upon request.	
Fraud prevention partners	Kount, Accertify, CyberSource, FICO, TSYS, Lean Industries, Pega Systems, ACI	
Other services	More information available upon request.	
Third party connection	More information available upon request.	
Technology: anti-fraud detection tools available		
Address verifications services	No	
CNP transactions	Yes	
Card Verification Value (CVV)	No	
Bin lookup	No	
Geo-location Checks	No	
Device Fingerprint	No	
Payer Authentication	No	
Velocity Rules – Purchase Limit Rules	No	
White list/black list database	No	
KYC – Know Your Customer	No	
Credit Rating	No	
Follow up action	Additional authentication (out of band authentication) and transaction verification capabilities	
Other		
Authentication Context		
Online	Yes	
Mobile	Yes	
ATM	No	
POS	No	

Call centre	
Other	More information available upon request.
Reference Data connectivity	
Connectivity to governmental data	No
Other databases	commercial attribute providers, e.g. credit databases
Fraud management system type	
Single-channel fraud prevention system	No
Multi-channel fraud prevention system	Yes
Certification	
Type	PCI. More information available upon request.
Regulation	PCI. More information available upon request.
Other quality programms	More information available upon request.
Other remarks	More information available upon request.
Clients	
Main clients / references	Our suite of services delivers significant revenue growth and cost saving opportunities to more than 5400 merchants in 40+ countries and more than 580 card issuers in 20+ countries. Seven of the top ten ecommerce brands, 14 of the top 20 North American card issuers, and two of the top five UK card issuers rely on Ethoca solutions and the network that powers them.
Future developments	Additional collaboration based solutions to stop friendly fraud, minimise false declines, and increase overall acceptance.



MAKE ECOMMERCE SIMPLY ABOUT COMMERCE

Fraud, chargebacks and false declines shouldn't drive a wedge between card issuers and merchants.

For far too long, ecommerce merchants and card issuers have been going it alone in the fight against fraud. With no proven, reliable way to communicate and collaborate, fraud losses rise unnecessarily – and so do chargebacks. Even worse, good customers and cardholders are wrongly declined. By coming together through Ethoca's Global Collaboration Network, card issuers and merchants are stopping more fraud, eradicating chargebacks, increasing transaction acceptance and improving the customer experience.

The process is simple. Every day, the world's leading card issuers send cardholder confirmed fraud and customer dispute data to Ethoca. We turn this data into actionable alerts and send it to thousands of merchants around the world within hours – not weeks later through the slow, outdated chargeback process. Now there is a window of opportunity for card issuers and merchants to stop fraud and chargebacks before they happen. With Ethoca, everyone sleeps easy – except the fraudsters.

5400+ Merchants | 580+ Card Issuers | 40+ Merchants

Isn't it time you joined the Ethoca Network?

www.ethoca.com | sales@ethoca.com

ethoca™

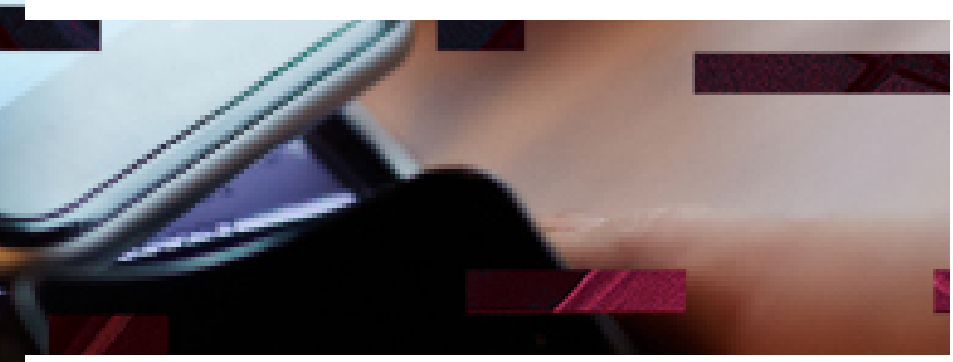
Company	Featurespace	View company profile in online database
FEATURE SPACE	Featurespace is the world-leader in Adaptive Behavioural Analytics and creator of the ARIC platform, a real-time machine learning software system for fraud management. ARIC monitors individual behaviours to catch new fraud attacks in real-time and reduce genuine transactions declined by 70%, which could save the payments industry USD 16bn annually.	
Website	www.featurespace.com	
Keywords for online profile	fraud, machine learning, analytics, customer friction, ARIC, adaptive analytics, real-time	
Business model	Licensed software	
Target market	Financial institutions, payment services providers, merchant acquirers, gambling, insurance	
Contact	info@featurespace.com	
Geographical presence	UK, Europe, USA	
Active since	2008	
Service provider type	Fraud detection, technology vendor	
Member of industry association and or initiatives	Merchant Risk Council, Network on Computational Statistics and Machine Learning	
Services		
Unique selling points	World-leading Adaptive Behavioural Analytics delivered via the machine learning ARIC platform. ARIC builds individual statistical profiles for every individual customer, spotting new fraud as it occurs, simultaneously reducing genuine transactions declined by over 70% and improving operational efficiencies over 50%; it uses in-session monitoring and link analysis to enable real-time customer understanding.	
Core services	Fraud prevention software, financial crime risk management, acceptance optimisation	
Pricing Model	Licence and support. For more information contact info@featurespace.com	
Fraud prevention partners	More information available upon request.	
Other services	payment acceptance optimisation, compliance product that identifies players at risk of gambling harm	
Third party connection	Ethoca, Emailage, Callcredit	
Technology: anti-fraud detection tools available		
Address verifications services	No	
CNP transactions	Yes	
Card Verification Value (CVV)	Yes - more details available on request	
Bin lookup	Yes - more details available on request	
Geo-location Checks	Yes - more details available on request	
Device Fingerprint	Yes	
Payer Authentication	No	
Velocity Rules – Purchase Limit Rules	Yes	
White list/black list database	Yes	
KYC – Know Your Customer	Yes - more details available on request	
Credit Rating	Yes	
Follow up action		
Other	Machine learning, behavioural analytics, in-session behaviour monitoring, link analysis, anomaly detection, sandbox functionality, deep learning models	
Authentication Context		
Online	Yes	
Mobile	Yes	
ATM		
POS	Yes	

Call centre	
Other	More information available upon request.
Reference Data connectivity	
Connectivity to governmental data	No
Other databases	No
Fraud management system type	
Single-channel fraud prevention system	Yes
Multi-channel fraud prevention system	Yes
Certification	
Type	More information available upon request.
Regulation	Regulated ICO under DPA
Other quality programms	PCI-DSS certified environment to process card data.
Other remarks	
Clients	
Main clients / references	TSYS, WorldPay, IATA, Betfair, Vocalink Zapp, Callcredit, GoHenry, Cashflows, MIT, Ally Bank
Future developments	More information available upon request.

FEATURE SPACE

OUTSMART RISK

Discover the ARIC™ Fraud Hub



- Stop fraud attacks in real-time and on any device
- Increase revenue – accept more genuine customers
- Reduce customer friction by over 70%

Discover the ARIC Fraud Hub:
www.featurespace.com

Featurespace is the world leader in Adaptive Behavioural Analytics, delivered via its machine learning ARIC™ platform.

Contact us:
info@featurespace.com

Gartner 2016 Cool Vendor · The FinTech50 2017 · Technology Fast 50 2016 UK WINNER Deloitte. · RED HERRING WINNER 100 EUROPE · THE SUNDAY TIMES TECH TRACK ONES TO WATCH 2015

Company	Feedzai	View company profile in online database
	Feedzai is AI. We're fighting fraud and coding the future of commerce with the most advanced risk management platform powered by big data and machine learning intelligence. Founded and developed by data scientists and aerospace engineers, Feedzai has one critical mission: make commerce safe. The world's largest banks, payment providers and retailers use Feedzai's machine learning technology to manage risks associated with banking and shopping, whether it's in person, online or via mobile devices. Feedzai is a US-based company and is funded by major venture capital investors including OAK HC/FT, Sapphire Ventures, Data Collective, and Citi Ventures. Learn more at www.feedzai.com.	
Website	www.feedzai.com	
Keywords for online profile	fraud detection, fraud prevention, machine learning, artificial intelligence, risk management	
Business model	On-premise, cloud, hybrid	
Target market	Online shoppers, financial institutions, issuers, merchants, acquirers, payment service providers, government services, online communities/web merchants, gaming and gambling, other online businesses	
Contact	sales@feedzai.com	
Geographical presence	Global	
Active since	2009	
Service provider type	Technology vendor, web fraud detection company	
Member of industry association and or initiatives	MRC	
Services		
Unique selling points	Feedzai makes commerce safe for business customers and creates a better experience for their consumers through artifcially intelligent machine learning. Financial services companies use Feedzai's anti-fraud technology to keep commerce moving safely.	
Core services	Artificial intelligence and machine learning based fraud detection platform for merchants, acquirers and issuers.	
Pricing Model	For more details contact our sales team at sales@feedzai.com	
Fraud prevention partners	Emailage, Socure, Deloitte, EnCap Security, Azul Systems, Cloudera, Datastax	
Other services	More information available upon request.	
Third party connection	More information available upon request.	
Technology: anti-fraud detection tools available		
Address verifications services	No	
CNP transactions	Yes	
Card Verification Value (CVV)	No	
Bin lookup	No	
Geo-location Checks	No	
Device Fingerprint	No	
Payer Authentication	Yes	
Velocity Rules – Purchase Limit Rules	Yes	
White list/black list database	Yes	
KYC – Know Your Customer	Yes	
Credit Rating	Yes	
Follow up action	Yes	
Other		

Authentication Context	
Online	Yes
Mobile	Yes
ATM	Yes
POS	Yes
Call centre	Yes
Other	More information available upon request.
Reference Data connectivity	
Connectivity to governmental data	
Other databases	More information available upon request.
Fraud management system type	
Single-channel fraud prevention system	Yes
Multi-channel fraud prevention system	Yes
Certification	
Type	PCIDSS Level 1
Regulation	Directive 95/46/EC
Other quality programms	More information available upon request.
Other remarks	
Clients	
Main clients / references	First Data, top-tier banks and merchants.
Future developments	More information available upon request.

feedzai

REAL ARTIFICIAL INTELLIGENCE

Every day, Feedzai's Agile Machine Learning protects over $3 billion in commerce.

Account Opening
Payment Authorization
Transaction Scoring
Merchant Onboarding
Loss Prevention

www.feedzai.com

Company	IdentityMind Global	View company profile in online database
	IdentityMind is the Trusted Digital Identity (TDIs) company. We offer a SaaS platform that builds, maintains and analyses digital identities worldwide. Our patented technology allows companies to perform identity proofing, risk-based authentication, regulatory identification and compliance, and ultimatelly detect and prevent synthetic identities, and stolen identities.	
Website	www.identitymindglobal.com	
Keywords for online profile	trusted digital identities, electronic DNA, eDNA	
Business model	Subscription-based, transaction-based	
Target market	Financial services companies, merchants	
Contact	evangelist@ientitymind.com	
Geographical presence	Global - offices in the US, Merico, UK and China	
Active since	2013	
Service provider type	Digital identity creation and analysis for risk and compliance	
Member of industry associations and intiatives		
Services		
Core services	Digital Identities for regulatory (KYC, AML, Sactions) and anti-fraud (onboarding, transaction) effectiveness	
Other services		
Unique selling points	Industry's most accurate risk scoring based on combination of KYC and fraud data, patented digital identity creation and analysis through patented eDNA	
Pricing model	Subscription-based, transaction-based	
Partners	We integrate with 40+ partners globally for Identity Proofing and more (e.g. Mitek)	
Offering: authentication technology used		
Technology used	Casandra, REST APIs	
Authentication context		
Online	Yes	
Mobile	Yes	
ATM	Yes	
Branch/Point of Sale	N/A	
Call Centre	N/A	
Other	N/A	
Issuing proces (if applicable)		
Assurance levels conformity	N/A	
Online issuing process (incl lead time in working days)	N/A	
Face-to-face issuing (incl lead time in working days)	N/A	
Issuing network	N/A	
Attributes offered		
Persons		
Companies		
Reference data connectivity		
Connectivity to governmental data	e.g. citizens register, company register, IDs	
Other databases	commercial attribute providers, e.g. credit databases	

Certification	
Type	PCI DSS 3.2, Privacy Shield
Regulation	
Other quality programs	
Other remarks	
Clients	
Main clients / references	Funding Circle, Goldmoney, Pontual, Silicon Valley Bank
Future developments	

IdentityMind™ GLOBAL

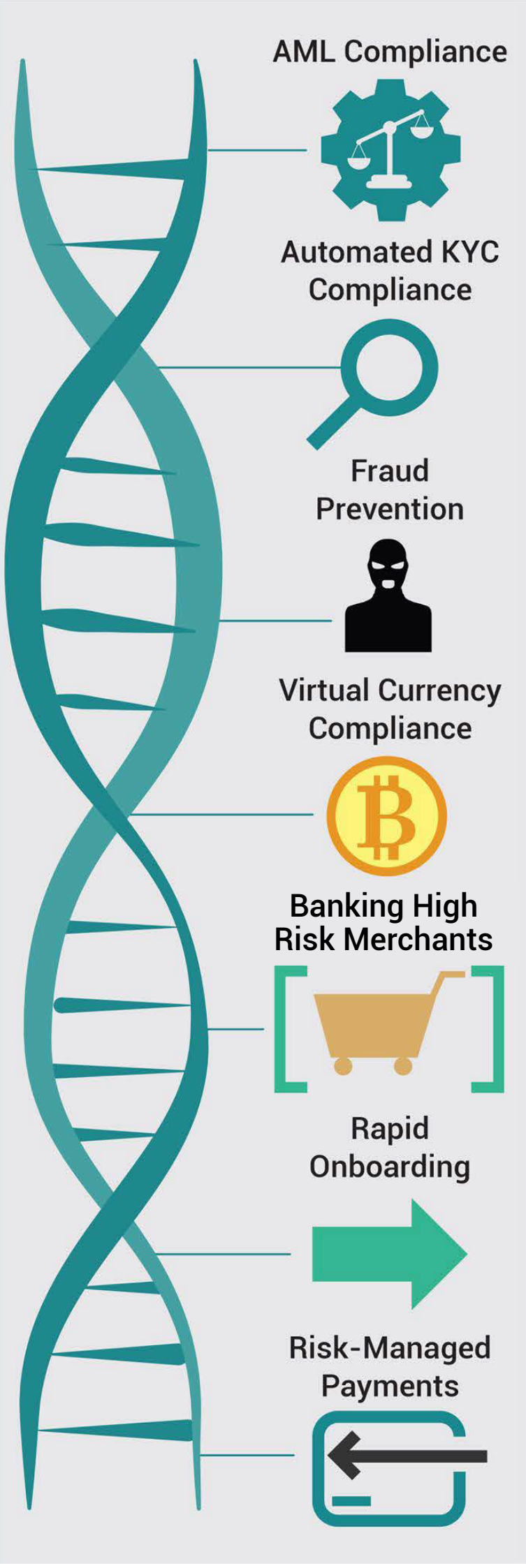
Digital Identities You Can Trust

Trusted Digital Identities: More Accurate Risk Management, More Efficient Compliance Operations

IdentityMind builds, maintains and analyzes digital identities worldwide, allowing companies to perform identity proofing, risk-based authentication, regulatory identification, and to detect and prevent identity fraud. Built-in transaction monitoring enables e-commerce fraud prevention, AML, and counter terrorism financing (CTF). Our patented eDNA™ tech tracks the entities involved in each transaction (e.g. onboarding, money transfers, online payments, etc.) to build reputations that can be anonymously shared across our Identity Network.

We've helped many companies address regulatory compliance and risk management concerns. We can help you too.

For more information, visit **http://www.identitymindglobal.com,** call us at 650.618.9977, or email us at **evangelist@identitymind.com**



Company	iovation Inc. View company profile in online database
	iovation protects online businesses and their end users against fraud and abuse, and identifies trustworthy customers through a combination of advanced device identification, multifactor authentication, shared device reputation, device-based authentication and real-time risk evaluation.
Website	www.iovation.com
Keywords for online profile	device identification, device reputation, online fraud prevention, online fraud detection, mobile fraud, account takeover prevention, device-based authentication, customer authentication, online reputation, multifactor authentication, device fingerprinting
Business model	SaaS
Target market	Online businesses, such as retailers, financial institutions, lenders, prepaid cards, insurers, social networks and dating sites, logistics, gaming/MMO, gambling operators, online auction sites, travel and ticketing companies
Contact	Connie Gougler, Director of Marketing, connie.gougler@iovation.com, 503-943-6748
Geographical presence	Global: iovation's business is 51% US and 49% international
Active since	2004
Service provider type	Device intelligence, fraud detection and prevention, customer authentication, multifactor authentication
Member of industry association and or initiatives	Merchant Risk Council, Online Lenders Association
Services	
Unique selling points	iovation provides a frictionless, flexible, reliable, real-time SaaS solution for user authentication and fraud prevention that tells our clients if a customer visiting their site is authorised for that account and/or is risky based upon specific criteria for evaluating the transaction or activity. iovation's global consortium contains the reputations of four billion devices and 45 million fraud events such as chargebacks, identity theft, account takeovers, online scams and many more.
Core services	iovation offers fraud prevention, customer authentication, multifactor authentication, and transaction reputation scoring.
Pricing Model	Per transaction fee based on system usage depending on volume, type of transaction, and length of contract.
Fraud prevention partners	Fiserv, Equifax, ID Analytics, Accertify, ACI Worldwide, Verisk, Callcredit, Imperva, Zoot
Other services	Our clients have access to the Fraud Force Community, an exclusive private B2B network of the world's foremost security experts sharing intelligence about cybercrime prevention, device identification, new threats and other fraud-related topics.
Third party connection	iovation delivers data in XML format and offers real-time APIs, allowing output to be integrated easily with third-party systems
Technology: anti-fraud detection tools available	
Address verifications services	No: While we do not offer AVS services, we capture the IP address and its geolocation of the device in the transaction. We can flag transactions from 'blocked' countries, as well as notify clients when mismatches occur between the IP address shown by the user's browser and the IP address we collect with our Real IP proxy unmasking feature.
CNP transactions	Yes: iovation's service is primarily used to detect high risk activity at login, account creation, fund transfer and checkout. In addition, our iovation score helps identify the most trustworthy customers in our clients' review queues so that they can take good business immediately, and offer higher-value promotions to their preferred customers.
Card Verification Value (CVV)	No: This service is handled through our client's payment processor.
Bin lookup	No: This service is handled through our client's payment processor.
Geo-location Checks	Yes: iovation's clients can flag transactions when activity is coming from an unauthorised country or through a proxy, and they can use our Real IP technology to pinpoint the user's actual location.
Device Fingerprint	Yes: iovation offers a defense-in-depth approach to device recognition, supporting native and web integrations for mobile, tablet and desktop devices.

Payer Authentication	No: This service is handled through our client's payment processor.
Device-based Authentication	Yes: iovation's authentication service allows clients to use their customer's known devices to help verify identity. Authentication happens in real-time, behind the scenes, reducing unnecessary friction.
Velocity Rules – Purchase Limit Rules	Yes: iovation's velocity rules flag transactions when thresholds are exceeded. These may include situations where too many accounts are accessed per device, or too many new accounts are created within a timeframe. Specific rules include accounts per device, accounts created per device, countries per account, countries per device, transactions per account, and transactions per device. Our service also flags transaction value thresholds, and other transactional velocities.
White list/black list database	Yes: iovation clients can flag transactions based on custom-built lists. These can be positive or negative lists. List types include accounts, devices, IP ranges, ISPs, locations and others, and are easily managed across rule sets.
Device Anomalies	Yes: iovation clients can flag transactions when device settings are anomalous and indicative of risk. While individual device characteristics may not be proof of risk, certain characteristics may be worth monitoring, and several in combination with each other may indicate attempts by the user to evade detection.
Fraud and Abuse Records	Yes: iovation clients can flag transactions that originate from an account or device already associated with fraud or abuse. Previous fraud or abuse is recorded in our system as evidence. The customer sets the types of evidence they want to consider, and decides whether to leverage only the evidence they log, or consider the evidence of other iovation subscribers.
KYC – Know Your Customer	No
Credit Rating	No
Follow up action	iovation's fraud prevention service provides an allow, review or deny result for each transaction. Clients then decide the best course of action to take in response to these results. iovation also returns detailed information about the device associated with the transaction; clients can store this data and correlate it back to identity management and other systems as needed.
Authentication Context	
Online	Yes
Mobile	Yes: iovation's mobile SDK for iOS and Android identifies jailbroken or rooted devices, and captures device location through IP address, network-based geo-location information, and GPS data. The location services expose mismatches between the reported time zone and location, long distances between transactions made in short periods of time, and other location-based anomalies. It also detects transactions originating from virtual machines or emulators.
ATM	Yes: iovation's device-based multifactor authentication solution can be used to facilitate the authentication of a person at an ATM
POS	Yes: iovation's device-based multifactor authentication solution can be used to facilitate the authentication of a person at POS
Call centre	Yes: iovation's device-based multifactor authentication solution can be used to facilitate the authentication of a person contacting a call centre
Reference Data connectivity	
Connectivity to governmental data	No
Other databases	MaxMind - IP geolocation
Fraud management system type	
Single-channel fraud prevention system	Yes: iovation delivers comprehensive online fraud prevention and customer authentication for mobile, tablet and PC-based transactions.
Multi-channel fraud prevention system	Our services focus on online transactions and complement a multi-channel prevention system.

Certification	
Type	
Regulation	iovation supports FFIEC compliance by providing device identification and device-based authentication services.
Other quality programms	iovation follows strict Quality Assurance processes for new products and services, and offers Service Level Agreements (SLAs), which include 99.9% uptime as a part of all customer agreements.
Other remarks	
Clients	
Main clients / references	NetSpend, Bazaarvoice, Intuit, CashStar, Aviva Insurance, New Era Tickets, AT&T Performing Arts Center, SG North and hundreds more.
Future developments	For more information, please contact iovation at info@iovation.com

Company	Kount — View company profile in online database
	Kount's award-winning fraud management, identity verification and online authentication technology empowers digital businesses, online merchants and payment service providers around the world. With Kount, businesses approve more orders, uncover new revenue streams, and dramatically improve their bottom line all while minimizing fraud management cost and losses. Boost Sales, Beat Fraud with Kount.
Website	www.kount.com
Keywords for online profile	fraud prevention, account takeover, payment security, ecommerce, machine learning, dynamic data, merchant network, increase sales
Business model	SaaS
Target market	ecommerce, financial institutions, payment services providers, online communities, web merchants, apparel, automotive, dating/social, digital streaming, electronics, food/beverage, health/beauty, home/kitchen, gaming/gambling, telecom, travel/leisure, other online businesses
Contact	fraudfighter@kount.com
Geographical presence	Worldwide
Active since	2007
Service provider type	SaaS technology vendor, web fraud detection company
Member of industry association and or initiatives	Merchant Risk Council, National Retail Federation, CPE Credit Certification by NASBA, Internet Merchants Retail Group, Global Retail Insights Network.
Services	
Unique selling points	Through Kount's global network and proprietary technologies in AI and machine learning, combined with policy and rules management, companies frustrate online criminals and bad actors driving them away from their site, their marketplace and off their network. Kount's continuously adaptive platform provides certainty for businesses at every digital interaction.
Core services	Kount's advances in both proprietary techniques and patented technology include: superior mobile fraud detection, advanced artificial intelligence, multi-layer device fingerprinting, IP proxy detection and geo-location, transaction and custom scoring, global order linking, business intelligence reporting, comprehensive order management, professional and managed services.
Pricing Model	Tiered SaaS-based pricing model
Fraud prevention partners	Channel Partners: BlueSnap, Braintree (a PayPal Service), Cayan, Chase, Conekta, Etisalat, Eway, First Atlantic Commerce, Global Payroll Gateway, J.P.Morgan, LimeLight, MaxiPago, Moneris, Openpay, PayCertify, Pinpoint Intelligence, Recurly, Sage. eCommerce Partners: 3dcart, demandware, Magento, mozu, Pulse Commerce, Xcart.
Other services	Chargeback managed services, underwriting, risk-based authentication, low-cost device fingerprinting, data orchestration, quarterly business review, policy/rules management, sales and marketing support (Kount Central Product), DataMart business intelligence, comprehensive onboarding and ongoing training support, dedicated client success manager, service support knowlege base.
Third party connection	BehavioSec, Chargebacks 911, Emailage, Ethoca, LexisNexis, Neustar, TeleSign, WhitepagesPro.
Technology: anti-fraud detection tools available	
Address verifications services	Yes
CNP transactions	Yes
Card Verification Value (CVV)	Yes
Bin lookup	Yes
Geo-location Checks	Yes
Device Fingerprint	Yes
Payer Authentication	Yes
Velocity Rules – Purchase Limit Rules	Yes

White list/black list database:	Yes
KYC – Know Your Customer	Yes
Credit Rating	No
Follow up action	Robust APIs and case management to trigger any type of follow up action.
Other	Complete case management, agent management and reporting, mobile SDK for superior device authentication, mobile app and mCommerce fraud prevention, supervised and unsupervised machine learning.
Authentication Context	
Online	Yes
Mobile	Yes
ATM	No
POS	Yes for internet-based
Call centre	Yes
Other	In-store kiosk, mail order, omnichannel.
Reference Data connectivity	
Connectivity to governmental data	Yes
Other databases	Emailage, WhitepagesPro, BehavioSec, Kount access device service.
Fraud management system type	
Single-channel fraud prevention system	Yes
Multi-channel fraud prevention system	Yes
Certification	
Type	PCI Compliance Level 1, SOC 2 Type 1, Privacy Shield, GDPR.
Regulation	More information available upon request
Other quality programms	More information available upon request
Other remarks	Contact fraudfighter@kount.com for more information
Clients	
Main clients / references	CD Baby, Dunkin' Brands, Hydrobuilder, Jagex, JOANN Fabric & Crafts, Leatherman, Micro Center, PetSmart, Staples, The Iconic, The Source, The Vitamin Shoppe, TickPick, WebJet, etc.
Future developments	Kount is continuously delivering net new functionality month after month, contact fraudfighter@kount.com for more information.

Increase Sales with Better Fraud Protection

Get back to business and let Kount take fraud off your hands.

Digital businesses using Kount have the confidence to grow boldly. How? Kount aggregates billions of transactions through its global network, feeding its AI and machine learning to expose fraud more accurately than other systems, in milliseconds. Weigh the value of each customer against potential fraud risk to maximize conversions with Kount.

Learn more about Kount's powerful tools for online retailers at **www.kount.com**

Kount®

Boost Sales. Beat Fraud.

Company	RISK IDENT	View company profile in online database
	RISK IDENT is an anti-fraud software development company based in the US and Europe that protects companies within the ecommerce, telecommunication and financial sectors. Our machine-learning software uses sophisticated data analytics to block payment fraud and account takeovers, all with human-friendly alerts that simplify a fraud prevention team's decision-making process.	
Website	www.riskident.com	
Keywords for online profile	online fraud prevention, account takeover prevention, device indentification, worlwide device pool, automatic fraud detection, fraud case processing, credit risk evaluation, mobile SDK	
Business model	Direct and through partners	
Target market	Online merchants, financial Institutions, payment services providers, online communities, gaming and gambling, other online businesses	
Contact	contact@riskident.com	
Geographical presence	Global	
Active since	2013	
Service provider type	Technology vendor, fraud detection	
Member of industry association and or initiatives	Merchant Risk Council	
Services		
Unique selling points	RISK IDENT battles payment fraud and account takeovers with a collection of highly developed software products that are easy to integrate. The software applies algorithms and machine learning on different data feeds to identify fraud risks on a variety of devices. FRIDA is an intelligent all-in-one solution that analyzes transactions using data analytics and machine-learning. It will continuously adapt to changing fraud patterns. DEVICE IDENT, a sophisticated device fingerprinting technology on the market, uses efficient rule sets that calculate a risk score to every device - including a SDK for native mobile applications. EVE is a flexible software platform that applies selected machine learning algorithms to evaluate different input streams for a real-time risk assessment - as a SaaS or on-premise solution.	
Core services	Fraud Detection and Credit Scoring Software. Device Fingerprinting Services.	
Pricing Model	Monthly licensing fees (FRIDA & EVE) / Per transaction (DEVICE IDENT)	
Fraud prevention partners		
Other services		
Third party connection	Yes	
Technology: anti-fraud detection tools available		
Address verifications services	Yes	
CNP transactions	Yes	
Card Verification Value (CVV)	-	
Bin lookup	Yes	
Geo-location Checks	Yes	
Device Fingerprint	Yes	
Payer Authentication	-	
Velocity Rules – Purchase Limit Rules	Yes	
White list/black list database	Yes	
KYC – Know Your Customer	Yes	
Credit Rating	Yes	
Follow up action	Various	
Other		

Authentication Context	
Online	Yes
Mobile	Yes
ATM	-
POS	Yes
Call centre	-
Other	
Reference Data connectivity	
Connectivity to governmental data	-
Other databases	Identity and Address Providers, Credit Scoring Providers
Fraud management system type	
Single-channel fraud prevention system	Yes
Multi-channel fraud prevention system	Yes
Certification	
Type	
Regulation	
Other quality programms	
Other remarks	Fully EU data privacy compliance
Clients	
Main clients / references	Key investor is Otto Group, Europes biggest online retailer
Future developments	

VIRTUALLY NO BUSINESS IS SAFE FROM FRAUD

Safeguard your enterprise and your customers by halting the sophisticated strategies of fraudsters and minimizing false positives – both of which boost sales.

RISK IDENT

We believe every business should have the most up-to-date technology in the fight against fraud. Stop fraudsters in their tracks and simultaneously create a better customer experience with RISK IDENT. As global experts with long-term experience in data science and machine learning, we offer highly efficient anti-fraud solutions that protect millions of transactions within the ecommerce, telecoms and financial services – each and every day.

www.riskident.com | contact@riskident.com

Company	SecuredTouch	View company profile in online database
	SecuredTouch is the leader in behavioral biometrics for mobile transactions, delivering continuous authentication technologies to strengthen security and reduce fraud while improving customers digital experience. Our mobile-optimised solutions require no enrollment, they are easy to implement, and provide real time alerts when suspicious activity is detected from login to logout.	
Website	www.securedtouch.com	
Keywords for online profile	Behavioral biometrics, continuous authentication, mobile fraud, biometrics, mobile banking, bot detection, emulator detection	
Business model	subscription-based	
Target market	Card issuers,business services (webmerchants, telco's, financial, transport)	
Contact	contact@securedtouch.com	
Geographical presence	Global	
Active since	2014	
Service provider type	Digital identity service providers, fraud detection	
Member of industry associations and intiatives	N/A	
Services		
Core services	Continuous authentication and fraud detection based on behavioral biometrics	
Other services	Detecting device emulators and non-human behavior	
Unique selling points	SecuredTouch behavioral biometrics overcomes the weaknesses of older authentication methods while ensuring strong and continuous authentication and a friction-free user experience. The mobile-optimised solutions require no enrollment, they are easy to implement, and provide real time alerts when suspicious activity is detected from login to logout.	
Pricing model	subscription-based	
Partners	Kaspersky lab, IBM mobile first, Transmit Security	
Offering: authentication technology used		
Technology used	Behavioral biometrics	
Authentication context		
Online	Yes	
Mobile	Yes	
ATM	via application	
Branch/Point of Sale	via application	
Call Centre	via application	
Other	N/A	
Issuing proces (if applicable)		
Assurance levels conformity	N/A	
Online issuing process (incl lead time in working days)	N/A	
Face-to-face issuing (incl lead time in working days)	N/A	
Issuing network	N/A	
Attributes offered		
Persons	N/A	
Companies	N/A	
Reference data connectivity		
Connectivity to governmental data	N/A	
Other databases	N/A	

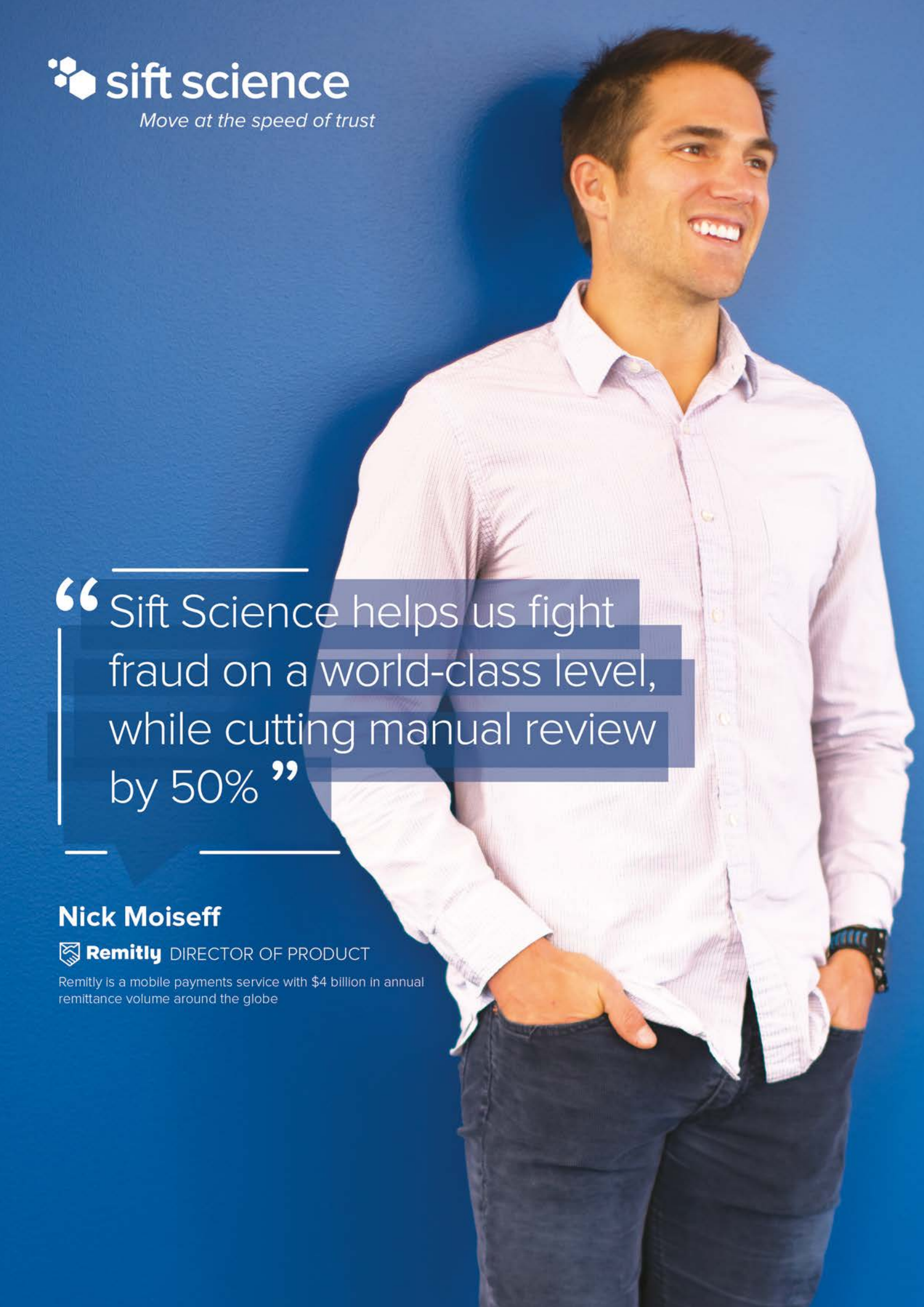
Certification	
Type	N/A
Regulation	PSD2
Other quality programs	Account takeover detection, automated fraud detection, risk-based authentication, RAT
Other remarks	
Clients	
Main clients / references	Banking, ecommerce
Future developments	IoT

Company	Sift Science	View company profile in online database
sift science *Move at the speed of trust*	Thousands of global businesses depend on the Sift Science Digital Trust Platform to determine in real time which users they can trust. Sift Science's Live Machine Learning, global trust network, and automation technologies fuel growth while protecting businesses and their customers from all vectors of fraud and abuse.	
Website	www.siftscience.com	
Keywords for online profile	fraud prevention, account takeover, content abuse, fraud detection, machine learning, ecommerce fraud, fraud prevention software	
Business model	SaaS	
Target market	ecommerce, financial institutions, payment services providers, online communities, web merchants, gaming and gambling, travel, on-demand services, online ticketing, marketplaces	
Contact	sales@siftscience.com	
Geographical presence	Global	
Active since	2011	
Service provider type	SaaS technology vendor, web fraud detection company	
Member of industry association and or initiatives	Merchant Risk Council	
Services		
Unique selling points	Live Machine Learning, global network, advanced automation	
Core services	A suite of products that prevent payment fraud, account takeover, content abuse, fake accounts, and promo abuse.	
Pricing Model	Pay as you go with volume discounts based on transaction volume.	
Fraud prevention partners	Soon	
Other services	Integration and support	
Third party connection	Contact us for more information.	
Technology: anti-fraud detection tools available		
Address verifications services	Yes	
CNP transactions	Yes	
Card Verification Value (CVV)	Yes	
Bin lookup	Yes	
Geo-location Checks	Yes	
Device Fingerprint	Yes	
Payer Authentication	No	
Velocity Rules – Purchase Limit Rules	Yes	
White list/black list database	Yes	
KYC – Know Your Customer	Yes	
Credit Rating	No	
Follow up action	Yes	
Other	Yes	
Authentication Context		
Online	Yes	
Mobile	Yes	
ATM	No	
POS	No	
Call centre	No	
Other		

Reference Data connectivity	
Connectivity to governmental data	No
Other databases	Multiple
Fraud management system type	
Single-channel fraud prevention system	No
Multi-channel fraud prevention system	Yes
Certification	
Type	Information Security (SOC 2 Type 2)
Regulation	N/A
Other quality programms	Contact us for more information.
Other remarks	Contact us for more information.
Clients	
Main clients / references	Airbnb, HotelTonight, Twitter, Remitly, Wayfair, Jet, OpenTable, Indeed, Twilio, Match.com, Zoosk, Indeed, Instacart, Zillow, SeatGeek, Despegar, Fareportal
Future developments	Expanding products and markets

sift science

Move at the speed of trust



"Sift Science helps us fight fraud on a world-class level, while cutting manual review by 50%"

Nick Moiseff

Remitly DIRECTOR OF PRODUCT

Remitly is a mobile payments service with $4 billion in annual remittance volume around the globe

Company	Signifyd	View company profile in online database
	Signifyd solves the challenges that growing ecommerce businesses persistently face: billions of dollars lost in chargebacks, customer dissatisfaction from mistaken declines, and operational costs due to tedious, manual transaction investigation. Signifyd is in use by multiple companies on the Fortune 1000 and Internet Retailer Top 500 lists.	
Website	www.signifyd.com	
Keywords for online profile	fraud, chargeback	
Business model	Guaranteed Fraud Protection as a service for ecommerce	
Target market	Online communities, web merchants, other online businesses	
Contact	sales@signifyd.com	
Geographical presence	US	
Active since	2011	
Service provider type	Technology vendor, web fraud detection company	
Member of industry association and or initiatives	MRC, NRF	
Services		
Unique selling points	As the world's largest provider of Guaranteed Fraud Protection, Signifyd provides a 100 percent financial guarantee against fraud and chargebacks on every approved order. This effectively shifts the liability for fraud away from ecommerce merchants allowing them to increase sales and open new markets while reducing risk.	
Core services	Data enrichment, risk score, guarantee decision, 48h payback for fraudulent chargebacks	
Pricing Model	Percentage of approved order for guaranteed protection (GMV)	
Fraud prevention partners	Accertify, Threatmetrix	
Other services	More information available upon request	
Third party connection		
Technology: anti-fraud detection tools available		
Address verifications services	Yes	
CNP transactions	Yes	
Card Verification Value (CVV)	Yes	
Bin lookup	Yes	
Geo-location Checks	Yes	
Device Fingerprint	Yes	
Payer Authentication		
Velocity Rules – Purchase Limit Rules	Yes	
White list/black list database	Yes	
KYC – Know Your Customer		
Credit Rating		
Follow up action		
Other		
Authentication Context		
Online	Yes	
Mobile	Yes	
ATM		
POS	Yes	
Call centre	Yes	
Other		

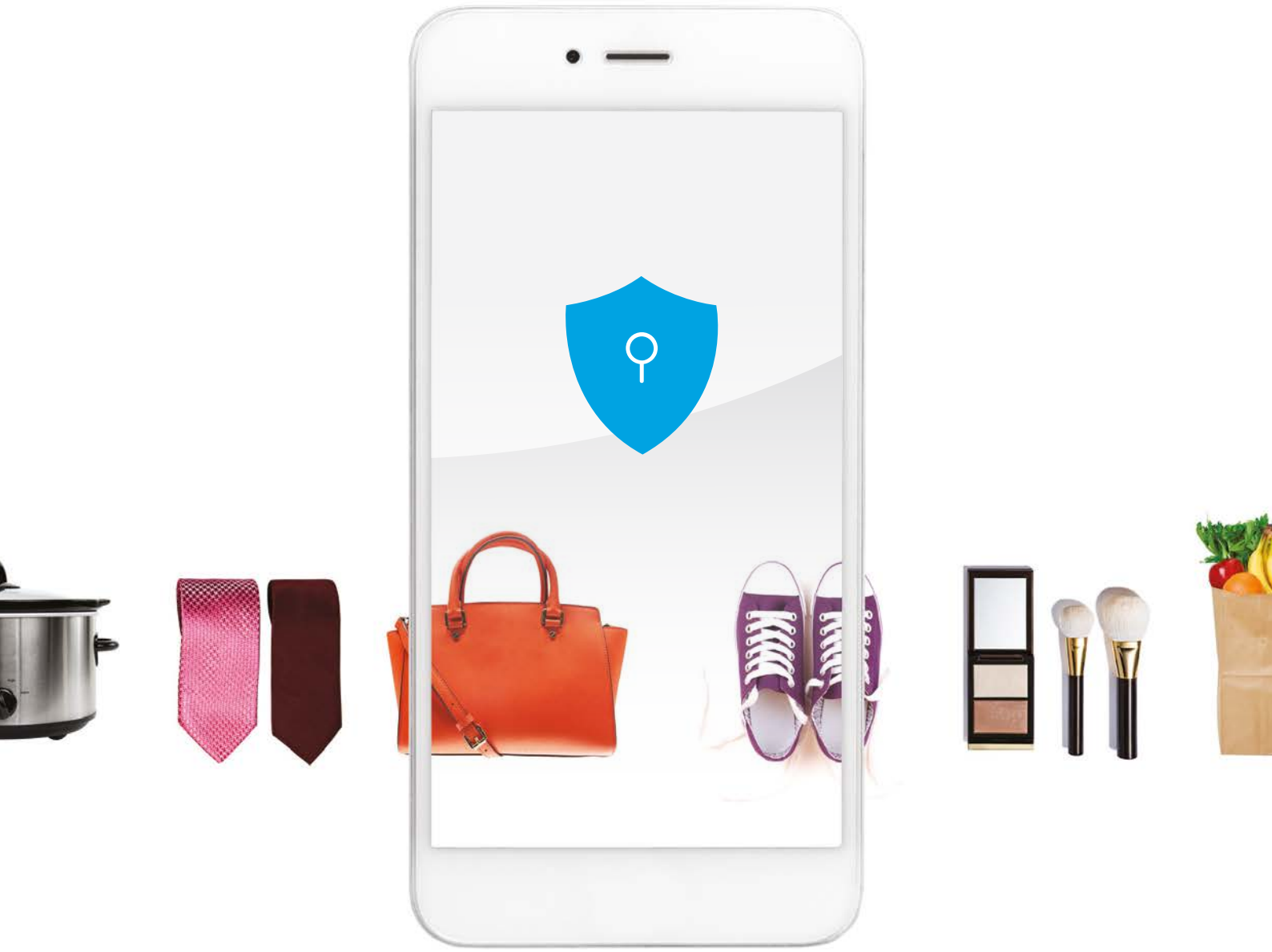
Reference Data connectivity	
Connectivity to governmental data	
Other databases	
Fraud management system type	
Single-channel fraud prevention system	Yes
Multi-channel fraud prevention system	Yes
Certification	
Type	PCI
Regulation	
Other quality programms	More information available upon request
Other remarks	More information available upon request
Clients	
Main clients / references	Build.com, Jet.com, Lacoste, Wayfair
Future developments	More information available upon request

SIGNIFYD

WWW.SIGNIFYD.COM

Guaranteed Fraud Protection

is changing e-commerce forever



Partner of the Year 2017 ThreatMetrix — Digital Identity Excellence Awards

SELECT MAGENTO TECHNOLOGY PARTNER

Gartner Cool Vendor 2017

Forbes FINTECH 50

CB INSIGHTS THE FINTECH 250

Company	Simility	View company profile in online database
	Simility provides intelligent fraud prevention that grows with you. Our flexible platform ingests data sources in the public or private cloud or on site. Plus, you can easily bring in new sources (whether structured, unstructured, or data lakes) as you grow. Without having to write a single line of code, your analysts can quickly and accurately identify evolving fraudulent tactics across silos and create appropriate rules, thanks to a powerful combination of human intelligence with Simility's self-optimising machine-learning models. Simility helps you spot and stop fraud in real time while providing greater fraud intelligence with fewer false positives.	
Website	https://simility.com/	
Keywords for online profile	Fraud detection, fraud prevention, anti-fraud, trust and safety, fraud fighting	
Business model	SaaS and on-premise models	
Target market	Online commerce, marketplaces, classifieds, financial services institutions (banks, mobile wallets, etc), payment service providers (acquirers, payment gateways, payment processors, ISOs/VARs), government services, online communities/web merchants, other online businesses: fintech	
Contact	contact@simility.com	
Geographical presence	Global coverage, with offices in Palo Alto (US), Dallas (US), Hyderabad (India), London (UK), Amsterdam (NL), and Sao Paulo (Brazil)	
Active since	2014	
Service provider type	Technology vendor, web fraud detection company	
Member of industry association and/or initiatives	Merchant Risk Council, SOC2 Type II compliant, PCI compliant	
Services		
Unique selling points	We offer an end-to-end fraud prevention platform combining device fingerprinting, risk engine driven by manual rules and machine learning models, and a case management workbench with advanced data visualisation capabilities. Simility's dynamic ontology provides centralised and flexible integration of structured and unstructured customer data to continuously detect and prevent the evolving fraud.	
Core services	Fraud detection, fraud prevention	
Pricing model	Per-transaction and on-premise license pricing models	
Fraud prevention partners	Assertiva, Pagar.me, Brinks	
Other services	Data Science as a Service	
Third party connection	Simility can connect to various 3rd party feeds, including those internal to our customers	
Technology: anti-fraud detection tools available		
Address verifications services	Yes	
CNP transactions	Yes	
Card Verification Value (CVV)	More information available upon request.	
Bin lookup	Yes	
Geo-location checks	Yes	
Device fingerprint	Yes	
Payer authentication	Yes	
Velocity rules – Purchase limit rules	Yes	
White list/black list database	Yes	
KYC – Know Your Customer	Yes	
Credit rating	More information available upon request.	
Follow up action	Yes	
Other	IP blacklists, device fingerprint, behavioral biometrics	

Authentication context	
Online	Yes
Mobile	Yes
ATM	More information available upon request.
POS	Yes
Call centre	More information available upon request.
Other	Branch banking data
Reference data connectivity	
Connectivity to governmental data	Yes
Other databases	Yes, we work with a variety of third party services.
Fraud management system type	
Single-channel fraud prevention system	More information available upon request.
Multi-channel fraud prevention system	Yes
Certification	
Type	SOC2 Type I and II, PCI compliance.
Regulation	More information available upon request.
Other quality programmes	More information available upon request.
Other remarks	More information available upon request.
Clients	
Main clients / references	Customers include Global 500 in financial services, ecommerce, payments, classifieds. Public references include Chime, Dice, NettiX, Semhora, and Big Basket.
Future developments	Further interactive data visualisation and out-of-the box integrations with new data sources.

Adaptive Fraud Prevention

THE INTELLIGENT FRAUD PREVENTION SOLUTION THAT ADAPTS TO DEVICES, BEHAVIOR, AND YOUR UNIQUE BUSINESS

As businesses evolve, so do fraudsters. That's why Simility provides intelligent fraud prevention that grows with you. Our flexible platform ingests data sources in the public or private cloud or on site. Plus, you can easily bring in new sources (whether structured, unstructured, or data lakes) as you grow.

Without having to write a single line of code, your analysts can quickly and accurately identify evolving fraudulent tactics across silos and create appropriate rules, thanks to a powerful combination of human intelligence with Simility's self-optimizing machine-learning models.

Simility helps you spot and stop fraud in real time while providing greater fraud intelligence with fewer false positives.

See for yourself how Simility can help your organization get better fraud insights by contacting us for a demo at www.simility.com/demo.

TYPICAL FRAUD SCENARIOS DETECTED

Account takeover (ATO)
Account origination fraud
Wire transfer fraud
Omnichannel fraud
CNP fraud
Promotion abuse
And more!

TECHNOLOGY HIGHLIGHTS

- ✓ **Superior machine learning**
- ✓ **Device fingerprint with fuzzy matching and clustering**
- ✓ **Advanced behavioral analytics**
- ✓ **Dynamic ontology based on data lakes**
- ✓ **Simple, intuitive workbench**
- ✓ **Near real-time sub-50 msec response times**

Schedule a demo at www.simility.com/demo

See how we can help you solve your unique fraud problems.

WWW.SIMILITY.COM

simility

Company	ThreatMetrix	View company profile in online database
	ThreatMetrix®, The Digital Identity Company®, empowers the global economy to grow profitably and securely without compromise. With deep insight into 1.4 billion anonymized user identities, ThreatMetrix ID™ delivers the intelligence behind 75 million daily authentication and trust decisions to differentiate legitimate customers from fraudsters in real time.	
Website	www.threatmetrix.com	
Keywords for online profile	Digital Identity, authentication, identity verification, fraud detection	
Business model	Cloud-based, Software as a Service (SaaS)	
Target market	Ecommerce – online shoppers, financial institutions, insurance, payment services providers, government services, online communities/web merchants, gaming and gambling, other online businesses	
Contact	Courtney Austin, Senior Director EMEA Marketing, ThreatMetrix	
Geographical presence	Worldwide – providing transactional services to more than 200 countries.	
Active since	2005	
Service provider type	Digital identity service provider, technology vendor, web fraud detection company	
Member of industry association and or initiatives	FIDO, One World Identity, MRC	
Services		
Unique selling point	ThreatMetrix ID is the world's first unique, anonymous customer identifier for all users on the ThreatMetrix Digital Identity Network. This technology features an interactive graph visualisation of attributes related to an individual's digital identity, a confidence score on the veracity of the ID and a trust score.	
Core services	Digital identity, risk-based authentication, identity verification, fraud prevention, mobile security	
Pricing Model	Tiered pricing based on transaction volume	
Fraud prevention partners	ACI, Cardinal Commerce, CyberSource, First Data, FIS, Fujisoft, Gemalto, LexisNexis, Nets, Paysafe and Worldpay.	
Other services	Prevention against account takeover, new account registration and payment fraud, strong authentication, behavioral analytics and machine learning, bot and remote access trojan detection, professional services	
Third party connection	Yes	
Technology: anti-fraud detection tools available		
Address verifications services	Yes	
CNP transactions	Yes	
Card Verification Value (CVV)	No	
Bin lookup	No	
Geo-location Checks	Yes	
Device Fingerprint	Yes	
Payer Authentication	Yes	
Velocity Rules – Purchase Limit Rules	Yes	
White list/black list database:	Yes	
KYC – Know Your Customer	Yes	
Credit Rating	No	
Follow up action	additional authentication (out of band authentication) and transaction verification capabilities	
Other	Carrier ID for strong mobile authentication	

Authentication Context	
Online	Yes
Mobile	Yes
ATM	No
POS	No
Call center	No
Other	No
Reference Data connectivity	
Connectivity to governmental data	Yes
Other databases	ThreatMetrix Digital Identity Network is one of the largest databases for monitoring customers providing global shared intelligence. Every day millions of consumer events are logged as well as thousands of high risk flags.
Fraud management system type	
Single-channel fraud prevention system	Yes
Multi-channel fraud prevention system	Yes
Certification	
Type	SOC-2 expected in 2018
Regulation	No
Other quality programs	No
Other remarks	No
Clients	
Main clients / references	Netflix, Lloyds Banking Group, Visa, Yandex.Money
Future developments	We follow an agile development schedule with a six week sprint cycle throughout the year.

ThreatMetrix

www.threatmetrix.com

The Decision Engine for Seamless Digital Business

Fighting fraud with digital identity intelligence from billions of transactions and a powerful decision platform.

ThreatMetrix Digital Identity Network®

Harness the power of global shared intelligence from the largest network of its kind.

24b	1.4b	4.5b	.8b	1.5b	185
annual network transactions	unique online identities	unique devices identified	unique email addresses	mobile devices	countries served globally

Company	Web Shield Limited® View company profile in online database
	Founded by highly-motivated, technology-affine professionals from the credit card and IT industries, at Web Shield we use our expertise in large-scale project management, system architecture design, software development and several investigation areas to perform risk assessments and persistent monitoring of legal entities.
Website	www.webshield.com
Keywords for online profile	On-boarding, underwriting, monitoring
Business model	On-demand and subscription service
Target market	Acquiring banks, payment service providers, financial institutions, online communities, web merchants, credit bureaus (qualitative data approach), gaming and gambling, law enforcement, detective agencies., other online businesses
Contact	compliance@webshield.com
Geographical presence	Leipzig, Warsaw, London
Active since	2011
Service provider type	SaaS vendor, training, consulting services
Member of industry association and or initiatives	Merchant Acquirers' Comittee, European Financial Coalition, Internet Watch Foundation, Electronic Transactions Association
Services	
Unique selling points	Web Shield provides you with the tools you need to protect your business from merchants involved in illegal or non-compliant activities. Our highly precise investigation solutions enable you to make informed decisions about prospective and existing clients, keeping your business out of risky situations – and saving you time and money.
Core services	Adaptable underwriting and monitoring solutions
Pricing Model	
Fraud prevention partners	
Other services	Training seminars for risk management, underwriting best practices and online investigation. Content violation detection for Cyberlockers.
Third party connection	CreditSafe, LexisNexis, iSignthis
Technology: anti-fraud detection tools available	
Address verifications services	Yes
CNP transactions	No
Card Verification Value (CVV)	No
Bin lookup	No
Geo-location Checks	Yes
Device Fingerprint	No
Payer Authentication	No
Velocity Rules – Purchase Limit Rules	No
White list/black list database	Yes
KYC – Know Your Customer	Yes
Credit Rating	Yes
Follow up action	
Other	
Authentication Context	
Online	Yes
Mobile	Yes
ATM	No
POS	No
Call centre	No
Other	

Reference Data connectivity	
Connectivity to governmental data	Yes
Other databases	commercial attribute providers, e.g. credit databases
Fraud management system type	
Single-channel fraud prevention system	Yes
Multi-channel fraud prevention system	Yes
Certification	
Type	
Regulation	
Other quality programms	Mastercard Merchant Monitoring Service Provider
Other remarks	
Clients	
Main clients / references	
Future developments	Organiser of the RiskConnect Networking Conference for Risk Professionals in Frankfurt a.M. (www.riskconnect2017.com)

Company	Worldline	View company profile in online database
worldline e-payment services	European leader in the payments and transactional services industry, Worldline delivers new-generation services for B2B2C industries. Worldline activities are organised around three axes: merchant services, mobility and e-transactional services and financial services. Worldline employs more than 9,400 people worldwide, with estimated yearly revenue of more than EUR 1.5 billion.	
Website	https://worldline.com/	
Keywords for online profile	online fraud prevention, risk management, authentication, biometry, e-identity, PSD2, artificial intelligence, digital banking	
Business model	BPO transactional or licensing	
Target market	Online shoppers, financial institutions, payment services providers, government services, health services, transport, merchant services, telcos, online communities/web merchants, gaming and gambling, other online businesses	
Contact	infoWL@worldline.com	
Geographical presence	Headquarters in France + Europe, APAC, India, Latam + operations in Africa	
Active since	1973	
Service provider type	Digital identity service provider, technology vendor, web fraud detection company, strong authentication services, payment service provider (PSP), issuer, acquirer, mobile payments, digital banking, e-transactional services	
Member of industry association and or initiatives	Acsel, AFTE, Berlin Group, CAPS, Concert International, EBG, Mobey Forum	
Services		
Unique selling points	Worldline 45 year's expertise secures your digital transactions. We design, build and run our own solutions to provide independent end-to-end services in fraud fighting on any channel and economic sector. It covers many kinds of strong authentication and risk management, with real-time fraud detection, based on Artificial Intelligence algorithms.	
Core services	New-generation services enabling the payments and transactional services industry to offer smooth and secure solutions to the end consumers	
Pricing Model	Based on processed service units	
Fraud prevention partners	Available on request	
Other services	Worldline can provide services on the full digital services value chain, including payments and non payment transactions.	
Third party connection	Hundreds of banks and thousands of merchants worldwide	
Technology: anti-fraud detection tools available		
Address verifications services	Available on request	
CNP transactions	Worldline provides an end-to-end service in fraud prevention and risk management, with real time fraud detection and Articificial Intelligence based algorythms. This also includes CNP transactions.	
Card Verification Value (CVV)	Yes	
Bin lookup	Yes	
Geo-location Checks	Possible	
Device Fingerprint	Yes for online services with security requirements	
Payer Authentication	Yes with WL Trusted Authentication	
Velocity Rules – Purchase Limit Rules	Yes	
White list/black list database	White lists and black lists are complementing the overall detection rules and models	
KYC – Know Your Customer	Yes	
Credit Rating	Not applicable	
Follow up action	Additional authentication (out of band authentication) and transaction verification capabilities	
Other	Contact us for a specific request	

Authentication Context	
Online	Yes
Mobile	Yes
ATM	Yes
POS	Yes
Call centre	Yes
Other	IVR
Reference Data connectivity	
Connectivity to governmental data	Yes
Other databases	commercial attribute providers, e.g. credit databases, health personal information
Fraud management system type	
Single-channel fraud prevention system	Yes
Multi-channel fraud prevention system	Yes
Certification	
Type	ISO 14000, 9001:2000, 9001:2008, 27001, 14641-1
Regulation	PCI DSS, PCI CPP, 3D-S, Instant Payments
Other quality programms	Available on request
Other remarks	N/A
Clients	
Main clients / references	Available on request
Future developments	Available on request

Let's make a safer transactional world

The digital economy is booming, fostered by PSD2 regulation. Worldline expertise and solutions enable you to implement the right strategy that efficiently fights fraud while protecting your customers' experience, whatever your activities.

Rely on a trusted partner

+3,5 billion controlled transactions

with a **detection rate** of risky transactions of **99,4%**

for **+ 120 banks** and **+ 200,000 merchants**

available **worldwide**

worldline.com

an atos company

worldline
e-payment services

Glossary

Glossary

A

Abuse list

Intelligence-sharing mechanisms used to widely disseminate tactical fraud intelligence like mule accounts, phishing sites, malware distribution sites, compromised websites, botnet IP addresses, compromised point-of-sale terminals, etc. Abuse lists may be private (available on subscription or as part of a larger fraud detection solution) or public.

Account takeover (ATO)

A form of identity theft where a criminal gains complete control of a consumer's account, such as obtaining the PIN or changing the statement mailing address and/or making unauthorised transactions.

Acquirer

An acquirer (acquiring or merchant bank) is a bank or financial institution that processes credit or debit card payments on behalf of a merchant. The term indicates that the merchant accepts or acquires credit card payments from the card-issuing banks within an association.

Address Verification System (AVS)

A service used to check the billing address of the credit card provided by the user with the address on file at the credit card company. AVS is widely supported by Visa, Mastercard, and American Express in the US, Canada and the UK.

Anti-Money Laundering (AML)

A set of procedures, laws or regulations designed to stop the practice of generating income through illegal actions. In most cases, money launderers hide their actions through a series of steps that make it look like money coming from illegal or unethical sources was earned legitimately.

AML Software

A type of computer programme used by financial institutions to analyse customer data and detect suspicious transactions.

Artificial Intelligence

The simulation of the processes of human intelligence by machines, especially computer systems. These processes include learning (the acquisition of information and rules for using the information), reasoning (using the rules to reach approximate or definite conclusions), and self-correction.

Assurance IQ

A term from Mastercard, which enables the exchange of vital information from the merchant about the circumstances of a transaction. This enables Mastercard to provide a blended risk score about the transaction to the issuer, enhancing confidence in the approval.

Authentication

A security measure that determines whether someone or something is, in fact, who or what it declares to be. An authentication process implies the verification of a cardholder with the issuing bank. Authentication often precedes authorisation (although they may often seem to be combined). The two terms are often used synonymously but they imply two different processes.

Authentication factor

A piece of information and process used to authenticate or verify the identity of an entity based on one or more of the following:

- Possession e.g., device signature, passport, hardware device containing a credential, private key;
- Knowledge e.g., password, PIN;
- Inherence e.g., biometric characteristic;
- Context e.g., behaviour pattern, geo-location.

Authenticator

A set of data presented as evidence of an asserted identity and/or entitlements.

Authorisation

Verifying that the entity initiating a transaction is entitled to perform that action.

B

Bank Identification Numbers (BIN)

The first six to eight digits on a credit card, which can be used to identify the issuing bank that issued the card. BINs are traditionally used by online merchants as a way to detect fraud by matching the geographic area where the cardholder is located to the geographic area identified in the Bank Identification Number.

Behavioural analytics

Data that is collected and analysed about a user's normal online/mobile activity patterns. By this way, anomalous activity is identified in order to determine if certain transactions align or not with the user's typical patterns of transacting.

Big Data

Large data sets that may be analysed computationally to reveal patterns, trends, and associations relating to human behaviour and interactions. By developing predictive models based on both historical and real-time data, companies can identify suspected fraudulent claims in the early stages.

Binding and activation of authenticator

Establishing an association between a credential and the entity to which it will be issued (binding), making it ready for use (activation).

Botnet

A network of computers that fraudsters have corrupted with hidden software to secretly send spam.

Bring your own authentication (BYOA)

A computing concept in which an employee-owned device, such as a key fob or smartphone, can be used to provide authentication credentials within a business environment.

Bring your own device (BYOD)

Bring your own device (BYOD) is an IT policy where employees are allowed or encouraged to use their personal mobile devices — and, increasingly, notebook PCs — to access enterprise data and systems.

Bring your own identity (BYOI)

An approach to digital authentication in which an end user's username and password is managed by a third party.

Bust-out fraud

A type of credit card fraud where an individual applies for a credit card, establishes a normal usage pattern and solid repayment history, then racks up numerous charges and maxes out the card with no intention of paying the bill.

C

Card capture device

A device inserted into an ATM card slot which captures the data contained on the card.

Card testing

Occurs when a fraudster uses a merchant's website to "test" stolen credit card information to determine if the card is valid. Fraudsters can purchase lists of credit card numbers online on the dark web at a low cost but often do not know if the cards they are purchasing are active. To test these cards, fraudsters often use automated bots and scripts to run many of these numbers through a merchant's checkout page. If a transaction is approved, the fraudster knows that the card is valid and can make fraudulent high-value purchases elsewhere.

Card-on-file (CoF)

Authorised storage of a consumer's payment credentials by a merchant, PSP, or WSP, that allows the consumer to conveniently make repeat or automatic purchases without the need to re-enter payment credentials each time.

Cardholder-not-present (CNP) fraud

Using stolen cards or card details and personal information, a fraudster purchases goods or services remotely – online, by telephone or by mail order.

Case management

In context of fraud management, it refers to the actions required to contain and remediate the impact of a detected fraud incident. Case management system refers to the ICT tooling used to automate routine follow-up activities and facilitate case management workflows.

Case management system

It is the workflow automation system that facilitates the structured investigation of suspected fraud incidents and remediation of confirmed fraud.

CCV

A unique check value encoded on the magnetic stripe and replicated in the chip of a card or the magnetic stripe of a Visa card to validate card information during the authorisation process.

CCV2 (CID)

Also known as Card Validation Code or Value, or Card Security Code. This is a unique 3-digit check value generated using a secure cryptographic process that is indent-printed on the back of a Visa card or provided to a virtual account holder.

CEO fraud

An e-mail scam in which the attacker spoofs a message from the boss and tricks someone at the organization into wiring funds to the fraudsters.

Change of address fraud

Occurs when the fraudster obtains details of a genuine customer's account and then contacts the business to announce that he has changed address. This is usually accompanied or followed by a request for items of value such as a chequebook, debit card or statement of account to be sent to the fake new address. A false change of address is used to facilitate previous address fraud and account/facility takeover fraud.

Chargeback

Chargeback occurs when a credit cardholder contacts their credit card issuing bank to initiate a refund for a purchase made on their credit card. Chargebacks are generally the result of a cardholder changing their mind, being dissatisfied with their purchase or a case of fraud. The fraud can result from the unauthorised use of their credit card (stolen card) or the cardholder purposely seeking to dispute a legitimate purchase they made (see 'delivery and returns fraud').

Chip Authentication Programme (CAP)

The CAP is a Mastercard initiative and technical specification for using EMV banking smartcards developed for authenticating users and transactions in online and telephone banking. It was also adopted by Visa as Dynamic Passcode Authentication (DPA). CAP is a form of two-factor authentication as both a smartcard and a valid PIN must be present for a transaction to succeed.

The CAP specification defines a handheld device (CAP reader) with a smartcard slot, a numeric keypad, and a display capable of showing at least 12 characters. Banking customers who have been issued a CAP reader by their bank can insert their Chip and PIN (EMV) card into the CAP reader in order to participate in one of several supported authentication protocols.

Clean fraud

Clean fraud leverages stolen credit card information. Criminals make purchases by accurately impersonating legitimate cardholders through the acquisition of extensive amounts of personal data.

Cloud-based solutions

Also called Software-as-a-service (SaaS), it is a software running on a shared server farm that provides shared processing resources and data to computers and other devices on demand.

Consumer authentication

The term used to describe tools intended to verify that the person making the transaction is actually the person authorised to do so, both in-person and card-not-present transactions.

Credentials

Data issued to an individual by a third party with a relevant authority or assumed competence, presented so as to provide evidence of a claim. A credential is a piece of information asserting to the integrity of certain stated facts.

Credit bureau

In the context of lending, it refers to an organization providing information on borrowing and bill-paying habits of an individual or company.

Credit card fraud

Fraud committed using a credit card or any similar payment mechanism as a fraudulent source of funds in a transaction. The purpose may be to obtain goods without paying, or to obtain unauthorised funds from an account. Credit card fraud is also an adjunct to identity theft.

Counterfeiting

The fraudulent reproduction of original documents/instruments in a manner that enables the fraudster to pass them off as genuine/original items.

Customer identity and access management (CIAM)

Consumer identity and access management (CIAM) is a sub-genre of traditional identity and access management (IAM). Traditional IAM systems are designed to provision, authenticate, authorise, and store information about employee users. User accounts are defined; users are assigned to groups; users receive role or attribute information from an authoritative source. They are generally deployed in an inward-facing way to serve a single enterprise.

However, many enterprises have found it necessary to also store information about business partners, suppliers, and customers in their own enterprise IAM systems.

CIAM goes beyond traditional IAM in commonly supporting some baseline features for analysing customer behaviour, as well as integration into CRM and marketing automation systems. Nevertheless, CIAM differs from CRM in that, with CRM systems, sales and marketing professionals counted upon to enter the data about the contacts, prospects, and track the sales cycle. The focus of CRM is managing all processes around the customer relationship, while CIAM focuses on the connectivity with the customer when accessing any type of systems, on premises and in the Cloud, from registration to tracking. With CIAM, to some extent similar kinds of information as in CRM systems can be collected, but the consumers themselves provide and maintain this information.

Customer due diligence

Identification and verification of customers and beneficial owners.

Cryptography

Protecting information or hiding its meaning by converting it into a secret code before sending it out over a public network.

D

Data breach

An incident in which sensitive, protected or confidential data has potentially been viewed, stolen or used by an individual unauthorise to do so. Data breaches may involve personal health information (PHI), personally identifiable information (PII), trade secrets or intellectual property.

Data capture

The action or process of gathering data, especially from an automatic device, control system, or sensor.

Data Security Standard (DSS)

The Payment Card Industry Data Security Standard (PCI-DSS) is a widely accepted set of policies and procedures intended to optimise the security of credit, debit and cash card transactions, and protect cardholders against misuse of their personal information.

Dark web

Fraudsters use the dark web, the portion of the Internet that can be browsed anonymously, to search for stolen identities and credit/debit card numbers to buy hacking tutorials or other malicious services.

Deep web

The deep web is Internet content not indexed by search engines. It includes work portals, academic databases and private members websites not publicly accessible. Estimates put the deep web at about 500 times the size of the public web, containing over 500 billion pages of content not indexed by Google. It is difficult to gauge the deep web's size, because it has been intentionally not indexed for public consumption.

Deep learning

Deep learning is an aspect of artificial intelligence (AI) that is concerned with emulating the learning approach that human beings use to gain certain types of knowledge. At its simplest, deep learning can be thought of as a way to automate predictive analytics.

Delivery and return fraud

Return fraud is the act of defrauding a retail store via the return process. There are various ways in which this crime is committed. For example, the offender may return stolen goods to secure cash, or steal receipts or receipt tape to enable a falsified return, or to use somebody else's receipt to try to return an item picked up from a store shelf. Return abuse is a form of "friendly fraud" where someone purchases products without intending to keep them.

Derived identification

Relying on the identification that took place at another instance, for example, a bank or governmental institution. Making use of derived identification also has its constraints. Next to that, it becomes less valuable if everyone makes use of derived identification. It also implies the prospect already needed to have an account at another bank.

Device fingerprinting

Device fingerprinting is a process by which a fingerprint of a connected device – desktop, tablet, smartphone, game console, etc. – is captured when visiting a website.

Device ID

It is the unique serial number or 'fingerprint' that a particular device has embedded in it. It can be the combination of several components (e.g. CPU + graphics card) and can include a threshold (i.e. less than 100% matching) to allow for partial upgrades, such as with the iPass (proprietary) solution.

Device cloning

This is when the fraudster makes a software image of the device in order to make it appear as the regular user on their own device. It looks the same from a software perspective and fools device fingerprinting solutions.

Denial of service attack (DoS)

An attack on a computer system or network that causes a loss of service to users. A network of computers is used to bombard and overwhelm another network of computers with the intention of causing the server to 'crash'. A Distributed Denial of Service (DDoS) attack relies on brute force by using attacks from multiple computers. These attacks can be used to extort money from the businesses targeted.

Digital identity

It is a collection of identity attributes, an identity in an electronic form (e.g. electronic identity).

Digital signature

A digital code (generated and authenticated by public key encryption) which is attached to an electronically transmitted document to verify its contents and the sender's identity.

DDoS Attack (Distributed Denial of Service)

DDoS is a type of DoS attack where multiple compromised systems, often infected with a Trojan, are used to target a single system, causing service disruption.

Dumpster diving

A fraudster goes through someone's garbage to try to find personal information to commit fraud. This is why it is important to shred any personally identifiable information before throwing it away.

E

E-ID services

Services for entity authentication and signing data.

Electronic Data Interchange (EDI)

It is an electronic communication method that provides standards for exchanging data. By adhering to the same standard, companies that use EDI can transfer data from one branch to another and even across the world.

Encryption

A method of coding data, using an algorithm, to protect it from unauthorised access. There are many types of data encryption, and they are the basis of network security.

End-to-end encryption

Uninterrupted protection of the integrity and confidentiality of transmitted data by encoding it at the start and decoding it at the end of the transaction.

Endpoint authentication

A security system that verifies the identity of a remotely connected device (and its user), such as a personal digital assistant (PDA) or laptop, before allowing access to enterprise network resources or data.

Endpoint protection

Endpoint protection refers to a wide range of solutions for protecting and/or detecting compromise of the end-user's computing device (desktop, laptop, mobile device, etc.). Endpoint protection solutions, in general, use one or more of the following techniques:

- Hardening: the solution blocks or otherwise eliminates commonly exploited vulnerabilities.
- Monitoring/Detection: the solution monitors the system and/or user behaviour and detects anomalies.
- Sandbox: the solution redirects any untrusted content to a sandbox environment that enables safe identification of malicious content.
- Anti-Virus solutions are an example of endpoint solutions that generally use a signature/rule based approach.
- Sensitive Information Protection solutions rely more on information classification and heuristics or machine learning-based algorithms for detection of abnormal information flows.
- Malware Protection solutions rely on a combination of one or more of the three techniques.

EMV

EMV (Europay-Mastercard-Visa) is a global standard for credit and debit cards based on chip card technology. The EMV cards make in-person transactions more secure, but increase the threat of fraud in card-not-present transactions because the chip is not involved in the transaction and provides no benefit when the card is not present.

Email tumbling

It is sequential email addresses. For example, organised fraud transactions assigned to johndoe01@, johndoe02@, johndoe03@, etc. is indicative of a fraudster automatically generating email addresses.

F

Face recognition

Biometric modality that uses an image of the visible physical structure of an individual face for recognition purposes.

False front merchants

Entities who hide the true nature of their businesses and sales of card-brand prohibited goods and services. These companies do not actually engage in selling what they claim during the merchant underwriting process, and usually are involved in illicit, illegal endeavours.

False positive

It occurs when a good transaction or order is rejected by either the issuer or the merchant, due to suspected fraud.

FIDO (Fast ID Online)

A set of technology-agnostic security specifications for strong authentication. FIDO is developed by the FIDO Alliance, a non-profit organisation formed in 2012.

Fraud apps

These are fraudulent apps that work in two ways:

- simulated ad interactions;
- intentionally misleading buttons or layouts.

In the simulated ad interactions, bots trigger ad activity. With the misleading buttons or layouts, developers create layouts that overlap ads with content so users will unintentionally click the ads. Users usually have no intention of clicking some of these ads but do so because the ads are so small that they tap them by mistake. Furthermore, these types of apps can contain more ads than they are usually allowed by their operating system to serve, or display ads outside of the screen view of an application.

Fraud detection

Tools and techniques used to detect 'acts of fraud'. It includes tools and techniques for: data analysis, data mining, rule based detection systems, supervised machine learning systems, and unsupervised machine learning systems.

Fraud management

Organisational processes to prevent, detect, contain and remedy fraud.

Fraud prevention

Processes, tools, and techniques used to prevent 'acts of fraud'. It includes communication and awareness, authentication, and other business processes controls.

Fraud screening

A checking system that identifies potentially fraudulent transactions. Fraud screening helps reduce fraudulent credit card transactions, eliminating the need for manual reviews, minimising bad sales and improving a company's bottom line.

Federated identity

A federated identity is the means of linking a person's electronic identity and attributes stored across multiple distinct identity management systems. Without federated identity, users are forced to manage different credentials for every site they use.

Related to federated identity is single sign-on (SSO), in which a user's single authentication ticket, or token, is trusted across multiple IT systems or even organisations. SSO is a subset of federated identity management, as it relates only to authentication and is understood on the level of technical interoperability which would not be possible without some sort of federation.

Fingerprint recognition

Biometric modality that uses the physical structure of the user's fingerprint for recognition. In most fingerprint recognition processes, the biometric samples are compressed in minutiae points that reduce the size of data and accelerate the process.

First-party fraud

Fraud committed against a financial institution by one of its own customers.

Forgery

The process of making or adapting documents, such as checks, with the intent to deceive.

Fraud ring

A group of people who commit fraud together.

Fraud score

A fraud score may be available during transaction authorisation. This is a number, usually between 0 and 1,000 that represents the overall fraud risk of a particular transaction. The higher the number, the riskier the transaction.

Friendly fraud

When a consumer (or someone with access to a credit card) makes a purchase and then initiates a chargeback, saying they did not make the purchase and/or did not receive the goods or services.

G

Geo Location Detection

Set of diverse and ideally automated tests that help fraud protection solutions assess the risk of fraud involved in a specific order passing through a merchant's website. These tests might include IP to Zip Code, IP to Billing Address, High IP Cross Referencing, IP Geo Location & Proxy Detection, and NPA NXX Area Code Web Service.

Geographical IP Detector (GID)

A web shop or a fraud protection solution equipped with a GID can easily locate the real physical (geographical) location of a device, by tracking its IP Address.

Ghost terminal

A skimming device made up of an ATM touch pad and reader which are placed over a legitimate ATM. Even if the reader obtains card information and PIN, it cannot process the transaction since the legitimate ATM does not function. The card number and PIN are then used to commit fraud.

Global Address Verification Directories

This feature enables fraud protection solutions compare the address introduced by the visitor with the existing address, detecting any fake data. It also helps e-merchants keep their customers easily reachable.

Guaranteed Fraud Prevention

A kind of insurance that transfers the impact of fraud losses from the insured entity (bank or processor or merchant) to a third party. This may be linked to the implementation of specific fraud prevention solutions.

H

Hash function

A function that can be used to map digital data of arbitrary size to digital data of fixed size. The values returned by a hash function are called hash values, hash codes, hash sums, or simply hashes. With Bitcoin, a cryptographic hash function takes input data of any size, and transforms it into a compact string.

Honeypot

A decoy computer system for trapping hackers. They are designed to purposely engage and deceive hackers and identify malicious activities performed over the Internet.

Host Card Emulation (HCE)

On-device technology that permits a phone to perform card emulation on an NFC-enabled device. With HCE, critical payment credentials are stored in a secure shared repository (the issuer data centre or private cloud) rather than on the phone. Limited use credentials are delivered to the phone in advance to enable contactless transactions to take place.

Hybrid detection system

Fraud detection system that uses both rule based and machine learning techniques.

I

Identification

Claiming of a certain identity by someone and/or something.

Identity

Set of attributes related to an entity that allow an entity to be uniquely recognised within a context.

Identity of Things (IDoT)

An area of endeavour that involves assigning unique identifiers (UID) with associated metadata to devices and objects (things), enabling them to connect and communicate effectively with other entities over the internet.

Identity Service Provider

An identity provider (IdP) is a system entity that creates, maintains, and manages identity information for principals while providing authentication services to relying party applications within a federation or distributed network.

It usually offers user authentication as a service. Relying party applications, such as web applications, outsource the user authentication step to a trusted identity provider. Such a relying party application is said to be federated, that is, it consumes federated identity.

An identity provider is considered a trusted provider that enables consumers to use single sign-on (SSO) to access other websites. SSO enhances usability by reducing password fatigue. It also provides better security by decreasing the potential attack surface.

Identity spoofing

Using a stolen identity, credit card or compromised username / password combination to attempt fraud or account takeover. Typically, identity spoofing is detected based on high velocity of identity usage for a given device, detecting the same device accessing multiple unrelated user accounts or unusual identity linkages and usage.

Identity theft

Identity theft happens when fraudsters access enough information about someone's identity (such as their name, date of birth, current or previous addresses) to commit identity fraud. Identity theft can take place whether the fraud victim is alive or deceased.

Identity verification

Checking the provided information about the identity with previously corroborated information and its binding to the entity.

Identity and Access Management (IAM)

The security and business discipline that enables the right individuals to access the right resources at the right time and for the right reasons. It addresses the need to ensure appropriate access to resources across increasingly heterogeneous technology environments and to meet increasingly rigorous compliance requirements.

Information sharing network

In the context of fraud management, it refers to a public or private service provider of one or more Abuse Lists.

InfoSec (information security)

The practice of defending information from unauthorised access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.

Integrator (Systems Integrator)

An entity that specialises in bringing together component subsystems into a whole and ensuring that those subsystems function together.

Intelligence

The gathering, assessment and dissemination of information that is valuable for fraud prevention and/or detection. Fraud intelligence can be strategic (activities of threat actors, etc.) and/or tactical (mule accounts, phishing sites, botnet IPs, etc.).

Internal fraud

Internal fraud occurs when a staff member dishonestly makes false representation, wrongfully fails to disclose information, abuses a position of trust for personal gain, or causes loss to others. Internal fraud can range from compromising customer or payroll data to inflating expenses to straightforward theft. Sometimes it is an unplanned, opportunistic attack purely for personal financial gain, but sometimes it is linked to a serious and organised criminal network, or even terrorist financing.

Internet of Things (IoT)

The network of physical objects that feature an IP address for internet connectivity, and the communication that occurs between these objects and other internet-enabled devices and systems.

IoT Botnet

A group of hacked computers, smart appliances and Internet-connected devices that have been co-opted for illicit purposes.

Interoperability

A situation in which payment instruments belonging to a given scheme may be used in other countries and in systems installed by other schemes. Interoperability requires technical compatibility between systems, but can only take effect where commercial agreements have been concluded between the schemes concerned.

Investment fraud

Investment fraud is any scheme or deception relating to investments that affect a person or company. Investment fraud includes:

- illegal insider trading
- fraudulent manipulation of the Stock Market
- prime bank investment schemes.

Issuer

A bank or financial institution that issues cards to consumers on behalf of the card networks (Visa, Mastercard). The issuing bank is also known as the credit or debit card company. The issuer acts as the middleman for the consumer and the card network by contracting with the cardholders for the terms of the repayment of transactions.

J

Jitter

ATM card processing technology designed to prevent card-present fraud by using an irregular card swipe motion (i.e. stop-start) to distort the magnetic stripe details that could be picked up by fraudulent card skimmers.

K

Key Stroke Logger

Hardware or software that records the keystrokes and mouse movements made on a particular computer. Hardware loggers can be placed by dishonest staff or unauthorised visitors. Software loggers can be installed in the same way, or more usually by malicious email or malware. Authorised key loggers may be used in order to facilitate an audit trail.

Keystroke Dynamics (typing dynamics)

The automated method of identifying or confirming the identity of an individual based on the manner and the rhythm of typing on a keyboard.

Know Your Customer (KYC)

The term refers to due diligence activities that financial institutions and other regulated companies must perform to ascertain relevant information from their clients for the purpose of doing business with them. Know your customer policies are becoming increasingly important globally to prevent identity theft, financial fraud, money laundering and terrorist financing.

L

Level of Assurance (LoA)

Degree of confidence reached in the authentication process that the entity is what it claims to be or is expected to be.

Liability shift

The liability for chargebacks resulting from fraudulent transactions moves from the merchant to the issuing bank when the merchant has authenticated the transaction using any of the 3-D Secure protocols. Without Consumer Authentication, merchants are liable for chargebacks.

M

Machine Learning System

Machine learning fraud detection systems use artificial intelligence solutions to detect 'acts of fraud'. These techniques fall under two main categories:

Supervised learning systems – these systems require training data sets to learn and use techniques like neural networks, bayesian models, regression models, statistical models, or a combination.

Unsupervised learning systems – these systems are able to identify potential fraud based on techniques like clustering, peer group analysis, breakpoint analysis, profiling or a combination.

Mail Order – Telephone Order (MOTO)

MOTO accounts are required when more than 30% of credit cards cannot be physically swiped. Merchants that have a MOTO merchant account usually process credit card payments by entering the credit card information directly into a terminal that contains a keypad, by using terminal software installed on a personal computer, or by using a "virtual" terminal that allows the merchant to use a normal web browser to process transactions on a payment service provider's website.

Malware

A software specifically designed to disrupt or damage a computer system.

Man-in-the-browser

A form of internet threat related to man-in-the-middle (MITM); it is a proxy Trojan that infects a web browser by taking the advantage of vulnerabilities in browser security to modify web pages or transaction content, or to insert additional transactions, all in a completely covert fashion invisible to both the user and host web application. A proxy Trojan is a virus which hijacks and turns the host computer into a proxy server, part of a botnet, from which an attacker can stage anonymous activities and attacks.

Man-in-the-middle

In cryptography and computer security, it is a form of active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker.

Manual review

A technique in which merchants use staff members to perform manual checks on orders to determine which orders are fraudulent.

Merchant account

A type of bank account that allows businesses to accept payments in multiple ways, typically debit or credit cards. A merchant account is established under an agreement between an acceptor and a merchant acquiring bank for the settlement of payment card transactions.

Money laundering

The process of concealing the source of money obtained by illicit means. The methods by which money may be laundered are varied and can range in sophistication. Many regulatory and governmental authorities quote estimates each year for the amount of money laundered, either worldwide or within their national economy.

Multi-factor authentication

An approach to security authentication, which requires that the user of a system provide more than one form of verification in order to prove their identity and gain access to the system. Multi-factor authentication takes advantage of a combination of several factors of authentication; three major factors include verification by something a user knows (such as a password), something the user has (such as a smart card or a security token), and something the user is (such as the use of biometrics).

N

Nonrepudiation

The ability to deny a false rejection or refusal of an obligation with irrefutable evidence.

O

One-time Password (OTP)

A password that can be used only once, usually randomly generated by special software.

Open Authorisation (OAuth)

An open standard for token-based authentication and authorisation on the Internet. It allows an end user's account information to be used by third-party services, such as Facebook, without exposing the user's password. OAuth acts as an intermediary on behalf of the end user, providing the service with an access token that authorises specific account information to be shared. The process for obtaining the token is called a flow.

OpenID

An open standard that describes how users can be authenticated in a decentralised manner, eliminating the need for services to provide their own ad-hoc systems and allowing users to consolidate their digital identities. Users may create accounts with their preferred OpenID identity providers, and then use those accounts as the basis for signing on to any website which accepts OpenID authentication.

On-premise Solutions

A software that is installed and runs on computers on the organisation's premises (in the building), rather than remotely, such as a server farm or cloud.

Out-of-band Authentication

The use of two separate networks working simultaneously to authenticate a user.

P

Passive authentication

A method where the user signs in through a Web form displayed by the identity provider and the user is requested to log in.

Payment Application Data Security Standard (PA DSS)

PA DSS is a system designed by the Payment Card Industry Security Standards Council and adopted worldwide. It was implemented in an effort to provide the definitive data standard for software vendors that develop payment applications.

The standard aims to prevent developed payment applications for third parties from storing prohibited secure data including magnetic stripe, CVV2, or PIN. In that process, the standard also dictates that software vendors develop payment applications that are compliant with the Payment Card Industry Data Security Standards (PCI DSS).

Payment Card Industry Data Security Standard (PCI-DSS)

A proprietary information security standard for organisations that handle branded credit cards from the major card schemes. The PCI Standard is mandated by the card brands and administered by the Payment Card Industry Security Standards Council. The standard was created to increase controls around cardholder data to reduce credit card fraud. Validation of compliance is performed annually, either by an external Qualified Security Assessor (QSA) or by a firm specific Internal Security Assessor (ISA) that creates a Report on Compliance (ROC) for organisations handling large volumes of transactions, or by Self-Assessment Questionnaire (SAQ) for companies handling smaller volumes.

Pharming

A type of online fraud where people are redirected from a real website to a website impersonating a real one, with malicious intent.

Phishing

A method which allows criminals to gain access to sensitive information (like usernames or passwords). It is a method of social engineering. Very often, phishing is done by electronic mail. This mail appears to come from a bank or other service provider. It usually says that because of some change in the system, the users need to re-enter their usernames/passwords to confirm them. The emails usually have a link to a page similar to the one of the real bank.

Public Key Infrastructure (PKI)

The infrastructure needed to support the use of Digital Certificates. It includes Registration Authorities, Certificate Authorities, relying parties, servers, PKCS and OCSP protocols, validation services, revocation lists. Uses include secure e-mail, file transfer, document management services, remote access, web-based transactions, services, non-repudiation, wireless networks and virtual private networks, corporate networks, encryption, and ecommerce.

Point-to-point encryption (P2PE)

A point-to-point encryption (P2PE) solution is provided by a third party solution provider, and is a combination of secure devices, applications and processes that encrypt data from the point of interaction (for example, at the point of swipe or dip) until the data reaches the solution provider's secure decryption environment.

A PCI P2PE solution must include all of the following:

- Secure encryption of payment card data at the point-of-interaction (POI)
- P2PE-validated application(s) at the point-of-interaction
- Secure management of encryption and decryption devices
- Management of the decryption environment and all decrypted account data

Use of secure encryption methodologies and cryptographic key operations, including key generation, distribution, loading/injection, administration and usage.

Privacy

Privacy is the ability of a person to control the availability of personal information and exposure of himself or herself. It is related to being able to function in society anonymously (including pseudonymous or blind credential identification).

Proofing

Identity proofing is a common term used to describe the act of verifying a person's identity, as in verifying the 'proof of an ID'. Other terms that describe this process include identity verification and identity vetting.

R

Ransomware

Ransomware is a type of malicious software from cryptovirology that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid. While some simple ransomware may lock the system in a way which is not difficult for a knowledgeable person to reverse, more advanced malware uses a technique called cryptoviral extortion in which it encrypts the victim's files, making them inaccessible, and demands a ransom payment to decrypt them.

Ransomware attacks are typically carried out using a Trojan that is disguised as a legitimate file that the user is tricked into downloading or opening when it arrives as an email attachment.

Real-time Risk Management

A process which allows risk associated with payments between payment system participants to be managed immediately and continuously.

Relying Party (RP)

A website or application that wants to verify the end-user's identifier. Other terms for this entity include 'service provider' or the now obsolete 'consumer'.

Retail Loss Prevention

A set of practices employed by retail companies to reduce and deter losses from theft and fraud, colloquially known as 'shrink reduction'.

Risk assessment

The process of studying the vulnerabilities, threats, and likelihood of attacks on a computer system or network.

Risk-Based Authentication (RIBA)

Risk-Based Authentication is where issuing banks apply varying levels of stringency to authentication processes, based on the likelihood that access to a given system could result in it being compromised. As the level of risk increases, the authentication process becomes more intense.

Rule based fraud detection

Rule based fraud detection systems use correlation, statistics, and logical comparison of data to identify potential 'acts of fraud' based on insights gained from previous (known) fraud incidents. They generally use traditional methods of data analysis and require complex and time-consuming investigations that deal with different domains of knowledge like financial, economics, business practices and behaviour. Fraud often consists of many instances or incidents involving repeated transgressions using the same method. Fraud instances can be similar in content and appearance, but usually are not identical. Rule based systems rely on identifying a known fraud pattern.

S

Scareware

A type of malware that displays pop-up window warnings of non-existent computer infections that tricks you into buying fraudulent “protection” software.

Smart card

An access card that contains encoded information used to identify the user.

Secure element

A tamper-proof Smart Card chip capable to embed smart card-grade applications with the required level of security and features. In the NFC architecture, the secure element will embed contactless and NFC-related applications, and is connected to the NFC chip acting as the contactless front end. The secure element could be integrated in various form factors: SIM cards, embedded in the handset or SD Card.

Security protocol

A sequence of operations that ensure protection of data. Used with a communications protocol, it provides secure delivery of data between two parties.

Security Threat and Risk Assessment

A method that identifies general business and security risks aiming to determine the adequacy of security controls with the service and mitigating those risks.

Security token (authentication token)

It is a small hardware device that the owner carries to authorise access to a network service. The device may be in the form of a smart card or may be embedded in a commonly used object such as a key fob.

Sensitive data

Information that relates to contact information, identification cards and numbers, birth date, social insurance number and other data that can be used for malicious purposes by cybercriminals.

SIM Cloning

A victim’s SIM card data, containing all of their phone’s data, is copied to a fraudster’s SIM so that the fraudster can impersonate them and access all incoming communication, as well as mobile banking. To keep personal information secure, users are advised to make sure they download the latest banking apps directly from the official websites, and be wary of using financial institution contact details from SMSes or emails, as well as confirming account details via email, SMS, or telephone. Also, if a user realises (s)he is not receiving calls or text notifications, (s)he may have fallen victim to a SIM card cloning scam.

Single Point of Purchase

The ability to detect whether a consumer’s card may have been compromised when an institution is experiencing a high volume of fraudulent transactions.

Smishing (SMS phishing)

A variant of phishing email scams that utilises SMS systems instead of sending fake text messages.

Signing (confirmation by customer)

Confirming a financial or non-financial transaction by verifying an entity’s identity in a manner that is non-repudiable (i.e. using one or more authenticators).

Skimming

Card skimming is the illegal copying of information from the magnetic strip of a credit or ATM card. It is a more direct version of a phishing scam. In biometrics and ID, it could be the act of obtaining data from an unknowing end user who is not willing to submit the sample at that time.

Social engineering

It is a non-technical method of intrusion used by hackers to commit fraud. It relies on human interaction and often involves tricking people into breaking normal security procedures. It is one of the greatest threats that organisations encounter today.

Social Security fraud

Occurs when a fraudster uses one's Social Security Number in order to get other personal information. An example of this would include applying for more credit in one's name and not paying the bills.

Spear phishing

An e-mail that appears to be from an individual or business that the user knows. In fact, the respective e-mail is from the same criminal hackers who want the user's credit card and bank account numbers, passwords, and the financial information on their PC.

Spoofs

Various scams in which fraudsters attempt to gather personal information directly from unaware individuals. The methods could include letters, telephone calls, canvassing, websites, e-mails or street surveys.

Strong Customer Authentication (SCA)

In accordance with EBA Consultation Paper, the authentication procedure shall result in the generation of an authentication code that is accepted only once by the payment services provider each time that the payer, making use of the authentication code, accesses its payment account online, initiates an electronic transaction or carries out any action through a remote channel which may imply a risk of payment fraud or other abuses.

Suspicious Transaction Reports (STR)

A report compiled by the regulated private sector (most commonly banks and financial institutions) about financial flows they have detected that could be related to money laundering or terrorist financing.

Synthetic ID Fraud

This type of fraud occurs when a fictitious identity is created, usually with a combination of real and fake information, and is used to obtain credit, make purchases and open accounts.

T

Threat

A threat consists of an adverse action performed by a threat agent on an asset. Examples of threats are:

- a hacker (with substantial expertise, standard equipment, and being paid to do so) remotely copying confidential files from a company network or from card;
- a computer malware seriously degrading the performance of a wide-area network;
- a system administrator violating user privacy;
- someone on the internet listening confidential electronic communication.

Third-Party Fraud

Fraud committed against an individual by an unrelated or unknown third-party.

Token

Any hardware or software that contains credentials related to a user's attributes. Tokens may take any form, ranging from a digital data set to smart cards or mobile phones. Tokens can be used for both data/entity authentication (authentication tokens) and authorisation purposes (authorisation tokens).

Tokenization

The process of substituting a sensitive data with an easily reversible benign substitute. In the payment card industry, tokenization is one means of protecting sensitive cardholder PII in order to comply with industry standards and government regulations. The technology is meant to prevent the theft of the credit card information in storage.

Transaction Authentication Number (TAN)

A type of single-use password used for an online banking transaction in conjunction with a standard ID and password.

Triangulation fraud

Considered as one of the most complex ecommerce attack methods, triangulation fraud involves three points.

- An unsuspecting customer who places an order on an auction or marketplace using some form of credit, debit, or PayPal tender.
- A fraudulent seller who receives the order and then places the order for the actual product with a legitimate ecommerce website using a stolen credit card.
- A legitimate ecommerce website that processes the criminal's order.

Trust

The firm belief in the competence of an entity to act dependably, securely, and reliably within a specified context.

Trusted Framework

A certification program that enables a party who accepts a digital identity credential (called the relying party) to trust the identity, security and privacy policies of the party who issues the credential (called the identity service provider) and vice versa.

Trusted Third-Party

An entity trusted by multiple other entities within a specific context and which is alien to their internal relationship.

Two-Factor Authentication (2FA)

Two-factor authentication is a security process in which the user provides two means of identification, one of which is typically a physical token, such as a card, and the other of which is typically something memorised, such as a security code.

U

Unique Identity

A set of identifiers/attributes forms a unique identity. Furthermore, an identifier, such as a unique number or any set of attributes, is capable of determining precisely who or what the entity is.

URL spoofing

This is an attempt to closely mimic the URL of another website. This makes the fraudulent website appear legitimate.

V

Validation

Confirming that information given is correct, often by seeking independent corroboration or assurance.

Verified by Visa

Verified by Visa provides merchants, acquirers and issuers with cardholder authentication on ecommerce transactions, by leveraging the 3-D Secure protocols. It helps to reduce ecommerce fraud by ensuring that the transaction is being initiated by the rightful owner of the Visa account. This gives merchants, acquirers, issuers and consumers greater protection on ecommerce transactions.

Vishing

The act of using the telephone in an attempt to scam the user into providing private information that will be used for identity theft. The scammer usually pretends to be a legitimate business, and fools the victim into thinking (s)he will profit.

Voice authorisation

An approval response that is obtained through interactive communication between an issuer and an acquirer, their authorising processors or stand-in processing, or through telephone, facsimile or telex communications.

Voice over IP (VoIP, or voice over Internet Protocol)

Refers to the communication protocols, technologies, methodologies and transmission techniques involved in the delivery of voice communications and multimedia sessions over Internet Protocol (IP) networks, such as the internet. Other terms commonly associated with VoIP are IP telephony, internet telephony, voice over broadband (VoBB), broadband telephony, IP communications and broadband phone.

W

Wire fraud

A financial fraud involving the use of telecommunications or information technology.

3D Secure 2.0

3D Secure (3DS) is the program jointly developed by Visa and Mastercard to combat online credit card fraud. To reflect current and future market requirements, the payments industry recognised the need to create a new 3D Secure (3DS) specification that would support app-based authentication and integration with digital wallets, as well as traditional browser-based ecommerce transactions. This led to the development of EMV 3D Secure – Protocol and Core Functions Specification v2.0.0 (EMV 3DS 2.0 Specification). The specification takes into account these new payment channels and supports the delivery of industry leading security, performance and user experience.

THE PAYPERS

Don’t Miss the Opportunity of Being Part of Large-Scale Payments Industry Overviews

Once a year, The Paypers releases four large-scale industry overviews covering the latest trends, developments, disruptive innovations and challenges that define the global online/mobile payments, e-invoicing, B2B payments, ecommerce and web fraud prevention & digital identity space. Industry consultants, policy makers, service providers, merchants from all over the world share their views and expertise on different key topics within the industry. Listings and advertorial options are also part of the Guides for the purpose of ensuring effective company exposure at a global level.

B2B Fintech: Payments, SCF & E-invoicing

Payment Methods

Online Payments and Ecommerce

Web Fraud Prevention & Online Authentication

For the latest edition, please check the Reports section