Strategies for Fighting Fraud in the Real-Time World

February 2021

ACI Worldwide
Real-Time Payments

Finextra

Executive Summary

Globally, electronic payment volumes continue to grow, and consumers and businesses are conducting more banking activity via online and mobile devices. Convenience is a core feature for consumers and corporates alike, but it must not come at the cost of security. In this fast-changing environment, the ability to detect and prevent payments fraud and financial crime is crucial; cybercrime is a growing threat and the perpetrators have identified payments as a highly profitable target area.

An increasing number of cybersecurity breaches are causing significant losses for banks and corporates across the world. In February 2016, a cyber heist at Bangladesh Central Bank resulted in a loss of $81 million and prevented another $850 million worth of transactions from being processed on the SWIFT network. Similarly, cybercriminals hacked the SWIFT system and stole $9 million from Ecuadorian bank Banco del Austro in May 2016.

In May 2017, the WannaCry ransomware attack affected more than 150 countries and 200,000 computers, as attackers demanded each of those affected to pay up to $300 worth of bitcoins to unlock their systems.

As a form of cybercrime, card payment fraud is one of the priority crime areas of the European law enforcement agency Europol. According to the organization, in 2012 the total value of transactions made by debit and credit cards issued within the Single Euro Payments Area (SEPA) amounted to €3.5 trillion. In the same period, criminals acquired €1.33 billion [2013: €1.44 billion] from payment card fraud. This represents 38 cents lost to fraud for every €1,000 worth of transactions. Credit and debit card payments and online fraud are highly profitable criminal activities that are increasingly dominated by card-not-present (CNP) transactions (such as online purchases).

The total value of fraudulent transactions conducted using cards issued within SEPA and acquired worldwide amounted to €1.44 billion in 2013, which represented an increase of 8% from 2012, according to the European Central Bank's **Fourth Report on Card Fraud**. As a share of the total value of transactions, fraud rose by 0.001 percentage point to 0.039% in 2013, up from 0.038% in 2012. However, as a share of total transactions, fraud is still below the level observed in 2009. In 2013, 66% of the value of fraud resulted from CNP payments, 20% from transactions at point-of-sale terminals and 14% from transactions at automated teller machines (ATMs).

Data on payments fraud in the EU is difficult to obtain, not reliable and not comparable across member states. This makes the creation of an accurate picture of payments fraud in the EU, including its size, components and development over time, very difficult.

In a survey for **World Payments Report 2017**, bank executives ranked distributed denial of service (DDoS) attacks (50%) and customer payments fraud (31.3%) as the top two security challenges they face. High global levels of card fraud place a significant cost burden on banks, hence its identification as a major concern. The increasing adoption of digital offerings in transaction banking is also giving rise to higher levels of payments fraud, making cybersecurity a top priority for banks and corporates.

The European Payments Council's (EPC's) December 2017 **Payment Threats and Fraud Trends Report** stated that the organization and sophistication of recent cyberattacks demonstrate greater professionalism of cybercriminals. The number of DDoS attacks were continuing and frequently attack the financial sector. "Social engineering attacks and phishing attempts are still increasing, and they remain instrumental often in combination with malware, with a shift from customers, retailers, SMEs to company executives, employees (through 'CEO fraud'), financial institutions and payment infrastructures," says the report. "More and more, mobile devices are becoming an attractive target for cyber criminals, along with the IoT devices. The adoption of cloud services and big data analytics technologies which results in data stored 'everywhere' are bringing new opportunities to businesses, but new risks, too."

Regarding payments fraud specifically, the EPC found that CNP and lost and stolen card fraud will continue to be the predominant drivers, while skimming remains most common fraud at ATMs. For SEPA credit transfer and direct debit transactions, the criminals' use of impersonationand deception scams, as well as online attacks to compromise data, continue to be the primary factors behind fraud losses. This is when criminals target personal and financial details which are used to facilitate fraudulent transactions.

1 The Impact of the Payment Services Directive: Opening Pandora's Box?

The revised Payment Services Directive (PSD2), which came into effect on January 13, 2018, will have a significant impact on Europe's payments market. It ushers in a new era of competition and potentially with it, new sources of fraud as the payments value chain is opened. In this environment, third-party providers (TPPs) can directly access bank customers' payments and account information, if permitted to do so by customers. However, this raises questions about data privacy and security; in an increasingly networked ecosystem, identifying attackers will be a challenge.

"Next to the threats, there is also a competitive market drive for user friendliness and simplicity, which leads to increased pressure on security resources and difficult trade-offs to be made by payment service providers (PSPs)," says the EPC. "The challenge will be to find the right balance between the user friendliness and the security measures needed."

Under PSD2, consumers can give retailers permission to access the money in their accounts directly, with no intermediary. Such a connection will be achieved using application programming interfaces (APIs), which allow retailers to connect directly to the financial institutions of their customers. There are questions about who has access to an individual's payments and purchase history. This is valuable information for both retailers and payment services, not to mention cyber criminals. Under PSD2, many customers may no longer log on to their banks' digital banking websites, reducing the amount of relevant data available to the banks.

Most online fraud schemes initially attempt to gain access to a victim's bank account. For this reason, PSD2 contains rules for strong customer authentication (SCA). It stipulates the mandatory use of two-factor authentication for most transactions.

The rules of the security game are changing fundamentally with PSD2, the General Data Protection Regulation and EU Network and Information Security Directive. The aim of these regulatory initiatives is to create standards for security. In the past, banks' fraud prevention systems tended to rely on the fact that customers interacted with them directly; a bank possessed all the information needed to establish whether a transaction was fraudulent. Online purchases were usually processed via an intermediary, such as PayPal, which obtained the funds from the consumer's bank account or nominated credit card.

In its regulatory technical standards (RTS) for SCA in PSD2, which were issued in November 2017, the European Commission (EC) stated that electronic payment services offered should be carried out in a secure manner, "adopting technologies able to guarantee the safe authentication of the user and to reduce, to the maximum extent possible, the risk of fraud". The authentication procedure should include, in general, transaction monitoring mechanisms to detect attempts to use a payments service user's personalized security credentials that were lost, stolen or misappropriated, and should also ensure that the payments service user is the legitimate user and therefore is giving consent for the transfer of funds and access to its account information through a normal use of the personalized security credentials.

The EC also specified that the SCA requirements should be applied each time a payer accesses its payments account online, initiates an electronic payments transaction or carries out any action through a remote channel that may imply a risk of payments fraud or other abuse, by requiring the generation of an authentication code, which should be resistant against the risk of being forged in its entirety or by disclosure of any of the elements upon which the code was generated.

SCA should be based on two-factor authentication, stated the EC: "Where payment service providers apply strong customer authentication… authentication shall be based on two or more elements which are categorized as knowledge, possession and inherence and shall result in the generation of an authentication code." The authentication code will be accepted only once by the PSP when the payer uses the authentication code to access its payments account online, to initiate an electronic payments transaction or to carry out any action through a remote channel which may imply a risk of payments fraud or other abuses.

PSPs are required to adopt security measures to ensure that:

- No information on any of the elements of an individual's personalized security credentials can be derived from the disclosure of the authentication code
- It is not possible to generate a new authentication code based on the knowledge of any other authentication code previously generated
- The authentication code cannot be forged Moreover, PSPs must ensure that the means of generating an authentication code includes each of the following measures:
- If authentication for remote access, remote electronic payments and any other actions through a remote channel has failed to generate an authentication code, it shall not be possible to identify which of the elements referred to was incorrect.
- The number of failed authentication attempts that can take place consecutively shall not exceed five within a given period.
- The communication sessions are protected against the capture of authentication data transmitted during the authentication and against manipulation by unauthorized parties.
- The maximum time without activity by the payer after being authenticated for accessing its payments account online shall not exceed five minutes.

In addition to SCA, PSPs should employ the following further security measures, under the term dynamic linking:

- The payer is informed of the amount of the payments transaction and of the payee
- The authentication code generated is specific to the amount of the payments transaction and the payee agreed to by the payer when initiating the transaction

- The authentication code accepted by the PSP corresponds to the original specific amount of the payments transaction and to the identity of the payee agreed to by the payer
- Any change to the amount or the payee results in the invalidation of the authentication code generated

Throughout all the phases of an authentication, PSPs are required to ensure the confidentiality, authenticity and integrity of the amount of the transaction and the payee and the information displayed to the payer.

Another issue the EC addressed in the RTS was the changing nature of fraud methods. It suggests that SCA requirements should allow for "innovation in the technical solutions addressing the emergence of new threats to the security of electronic payments". To ensure that the requirements to be laid down are effectively implemented on a continuous basis, it is also appropriate to require that the security measures are documented, periodically tested, evaluated and audited by auditors with expertise in IT security and payments and operationally independent.

Against this background, providing a secure infrastructure to TPPs will be a challenge for banks. To prevent fraud in real time, most banks use packaged software whose fraud scoring models are trained over a period of 18 to 24 months. However, after PSD2 enables new transactions through TPPs, it will take around two years for the banks to generate scores reflecting the transaction risk. In the interim, banks' fraud analytics departments must perform proactive transaction monitoring and develop their own rules to prevent fraudulent transactions. Under PSD2, banks can block thirdparty access to accounts if they have the evidence that the activity is unauthorized or fraudulent. This is a capability they may well need to exercise in the PSD2 environment.

2 KYC and AML Obligations

In addition to a PSP's obligation to prevent fraudulent transactions, a growing requirement is to ensure transactions are not connected with money laundering, terrorist financing or are being perpetrated by the subject of sanctions. This is a serious concern as the fines for violating anti-money laundering (AML), know your customer (KYC) or sanctions rules are very high and during the past few years have totaled billions of dollars. For example, in late December 2017, U.S. bank Citi was fined $70 million by the U.S. Office of the Comptroller of the Currency for shortcomings in its AML policies.

The European Union's fourth AML Directive, which came into effect in mid-2017, requires ongoing KYC due diligence together with continuous transaction monitoring. The Directive applies to a range of businesses including banks, credit institutions, other financial institutions and businesses that make or receive cash payments for goods worth at least €10,000—irrespective of whether payment is made in a single or series of transactions. The Directive covers risk assessment and the corresponding risk approach, creation of national central registers of beneficial owners and waivers on customer due diligence for certain eMoney products.

An amendment to the Fourth AML Directive, called the Fifth AML Directive, aims to fill some gaps by regulating many financial means used by terrorists, from cash and trade in cultural artifacts to virtual currencies and anonymous prepaid cards. Virtual currency exchange platforms will be brought under the scope of the Fourth AML Directive to help identify the users who trade in virtual currencies. In addition, the EC will examine the possibility of applying the licensing and supervision rules of the PSD to virtual currency exchange platforms, as well as virtual wallet providers.

PSD2's SCA requirements are aimed at ensuring KYC processes guarantee the identification, and thereby know the identity, of the customer before transacting a payment. If that is absent, the transaction becomes invalid because it's not possible to verify whether it was the client who provided the authorization.

Accurate customer identification and authentication is crucial in a regulatory environment where violations of sanctions and AML and KYC rules can attract multi-million pound fines and damage reputations. Financial institutions are typically responsible for performing initial KYC screening whenever individuals, legal entities or correspondent banks open accounts or execute high-risk transactions. KYC is a broad term and includes the identification of the client profile and an understanding of their business. As sanctions are increasingly imposed, financial institutions must not only know their customer, but also know their customer's customers.

U.S. bank Citi describes the KYC process as "a costly and administrative-intensive exercise for banks, each satisfying its own requirements with thousands of employees conducting due diligence, document collection and data entry". However, given that all banks use the same types of data and interact with the same clients, there is an opportunity to reduce costs by engaging third-party data aggregators, or KYC utilities, that provide this service to all banks, says Citi. Consultancy PwC says centralizing the collection of customer information into a common repository that is accessible to participating financial institutions eliminates duplicative KYC activities across the industry. "This can yield significant cost efficiencies, improve customer service, allow for earlier revenue recognition and increase standardization of KYC quality and compliance."

KYC utilities are facilities managed by third-party platforms that aim to streamline the collection and exchange of data between banks and their clients, while maintaining appropriate privacy controls. Technology providers, consultancies, data providers and others have formed partnerships to offer utility KYC services.

Among the services is SWIFT's KYC Registry, which was launched in December 2014 and now has more than 3,000 banks in 175 countries exchanging their KYC data on it. The Registry was developed to provide SWIFT members with a costeffective, secure and easy-to-use way to exchange standardized KYC data with correspondents.

3 The Role of Technology in Tackling Payments Fraud

In tackling payments fraud, PSPs are increasingly turning to technology. Artificial intelligence and big data analytics to monitor and respond to fraud events without human intervention are emerging as an important weapon in the fight against fraud. To stop fraud in an ever-changing environment where fraudsters evolve and adapt to new technologies such as EMV, PSPs need tools that:

+ Are easy to deploy and manage
+ Work at the speed of fraudster innovation
+ Reduce costs

Successful fraud prevention is all about decisionmaking—accepting the good transactions and denying the fraudulent ones—with the best available information in real time. A winning fraud prevention solution allows revenues to grow and costs to shrink, ideally giving PSPs the ability to focus upon what they do best.

Westpac New Zealand believes real-time fraud detection will become a competitive differentiator in the future. The bank uses AI and machine learning to pattern match transactions. Long term, it hopes its customer will become "part of the intelligence" to identify transactions that have been flagged as fraudulent, says Dawie Olivier, Chief Information Officer at the bank[1]. Olivier says with real-time payments, the opportunity for fraud will be more frequent while the chances of recovering funds will be lower, given that real-time payments will also be settled in real time.

In late 2016, MasterCard announced Decision Intelligence, a machine-learning-based decision and fraud detection service. The solution uses AI technology to help financial institutions increase the accuracy of real-time approvals of genuine transactions and reduce false declines.

Previously, decision-scoring products were focused primarily on risk assessment, working within predefined rules. Decision Intelligence takes a broader view in assessing, scoring and learning from each transaction. That score then enables the card issuer to apply the intelligence to the next transaction.

Ajay Bhalla, president of enterprise risk and security, MasterCard, said when Decision Intelligence was launched: "We are solving a major consumer pain point of being falsely declined when trying to make a purchase. By using AI technology on our global network, we're helping financial institutions and merchants improve approval rates—and the consumer experience."

Building on other proprietary services, Decision Intelligence uses sophisticated algorithms to provide a predictive score to the issuer, based on intelligent analysis. The information is incorporated into their existing fraud mitigation efforts. Alternatively, issuers can activate the holistic MasterCard tool, which makes data-driven, real-time decisions tailored to the account, including defined alert and decline thresholds.

The technology behind Decision Intelligence examines how a specific account is used over time to detect normal and abnormal shopping spending behavior. In doing so, it leverages account information such as customer value segmentation, risk profiling, location, merchant, device data, time of day and type of purchase made.

In China, Alibaba has built a fraud risk monitoring and management system based on real-time big data processing and intelligent risk models. The system captures fraud signals directly from the huge amount of data the company holds on user behavior and analyzes them in real time using machine learning. The system identifies the bad users and transactions. To extend the fraud risk prevention ability to external customers, Alibaba has built a big data-based fraud prevention product called AntBuckler, which aims to identify and prevent all flavors of malicious behavior with flexibility and intelligence for online merchants and banks.

Alibaba deploys a multiple-layer fraud detection system. It has five checking layers to prevent fraud: account, device, activity, risk strategy and manual review. A fraudster may pass the first layer, but still must negotiate the next four layers.

Another very high-profile technology, blockchain, is still in a nascent stage with its potential as an enabler of digital identity and payments transaction security still being tested, says WPR 2017. Banks can leverage the technology to differentiate themselves in the provision of digital identity, authentication and KYC services. Banks are investing in projects that combine advanced cryptography that supports private or permission use of blockchain technology with transaction security elements that provide greater transaction visibility. To ensure the highest levels of cybersecurity and transaction security, all the ecosystem participants must assess security from multiple sources in the network.

The Report states: "Common security standards and protocols when developing and investing in new technologies and monitoring tools will be increasingly important as collaboration increases. With a common network governing the interfaces between banks and TPPs, various groups are looking to develop network-based security standards to ensure a secure environment is built around the dynamic payments ecosystem."

A useful approach is risk-based authentication (RBA) to detect the risk profile of transaction banks and retailers. Using the RBA and analytics processes, banks can create a threat matrix of fraud profiles to triangulate the threat instances to their origin and be able to proactively block fraudulent traffic. Behavioral analytics, AI, machine learning and threat matrix can help to continuously monitor the payments network and provide threat intelligence. Banks can undertake various activities such as continuously checking all systems for possible threats, observing markets, scenario simulation, examination of previous attacks, monitoring activities and applications, and establishing a payments control center to permanently monitor payments and identify exceptional situations.

4 Towards a Collaborative Future in the Fight Against Fraud

Financial institutions have realized that tackling such huge responsibilities as KYC, AML and fighting payments fraud on their own doesn't make sense. Moreover, fraud prevention requires more than technology alone. An important aspect to mitigate the risks related to payments is the sharing of fraud intelligence and information on incidents among PSPs.

A much more collaborative approach, based on information sharing, has emerged. Marco Doeland, Head of Risk Management at the Dutch Payments Association, believes collaboration and the sharing of information help reduce payment transactions fraud. In a January 2017 paper outlining how the country had significantly reduced fraud levels in online banking and payment cards transactions, he described the "Dutch model":

+ Agreement that banks will not compete on security
+ Information exchange between banks
+ Collaboration between banks, to include the shared delivery of products and services
+ Collaboration between banks and public and private sectors
+ Strong technical security measures

There are obstacles to such an approach elsewhere in Europe, he pointed out. For example, legislation can prove a hindrance to information sharing, particularly those related to privacy issues. Additionally, many European countries view anticartel legislation as a barrier to the sharing of information or to improved collaboration.

5 Conclusion

The tougher regulatory environment and the increasing sophistication of fraudsters mean PSPs face a considerable challenge in fighting payments fraud. But the technologies and techniques exist to create effective fraud prevention systems that are far more advanced than the legacy practices of the past.

When mapping out a strategy for real-time payments fraud protection, PSPs should include the following elements:

+ Adaptive machine learning. This facilitates realtime reaction and adaptation to new fraud signals, driving fast decision making and responses to emerging fraud threats. Solutions should be designed to incorporate fraud and payments data through proprietary or third-party modeling and analytic capabilities.
+ Shared intelligence approach to leverage crossindustry knowledge and data. By leveraging crossindustry knowledge and data, PSPs can reduce the resources and time they require to develop strategies. Fraud is not a competitive area; it is best tackled collaboratively.
+ Real-time payments fraud screening. PSPs should consider developing real-time detection and prevention techniques for enterprise risk management. Such techniques should be based on the collective expertise of vendors, issuers, acquirers, merchants, processors and card networks.
+ Integrated payment engines. Payment engines should be integrated with fraud processing in a way that allows for both existing and emerging payment mechanisms to be covered.

By gaining a holistic view of transactions and activities with a standardized approach that reaches across all lines of business, PSPs can effectively tackle payments fraud.

Discover the exponential growth of real-time payments in your market and consider the impact on fraud prevention. Read the report, "Prime Time for Real-Time".

Download Report

[1] For more on what Westpac New Zealand has done with real-time fraud detection, visit: https://www.aciworldwide.com/insights/videos/2017/october/westpac-new-zealand-uses-artificial-intelligence-machine-learning--pattern-matching-features-of-acis

ACI Worldwide is a global software company that provides mission-critical real-time payment solutions to corporations. Customers use our proven, scalable and secure solutions to process and manage digital payments, enable omni-commerce payments, present and process bill payments, and manage fraud and risk. We combine our global footprint with local presence to drive the real-time digital transformation of payments and commerce.

LEARN MORE

www.aciworldwide.com
@ACI_Worldwide
contact@aciworldwide.com

Americas +1 402 390 7600
Asia Pacific +65 6334 4843
Europe, Middle East, Africa +44 (0) 1923 816393

ACI Worldwide
Real-Time Payments