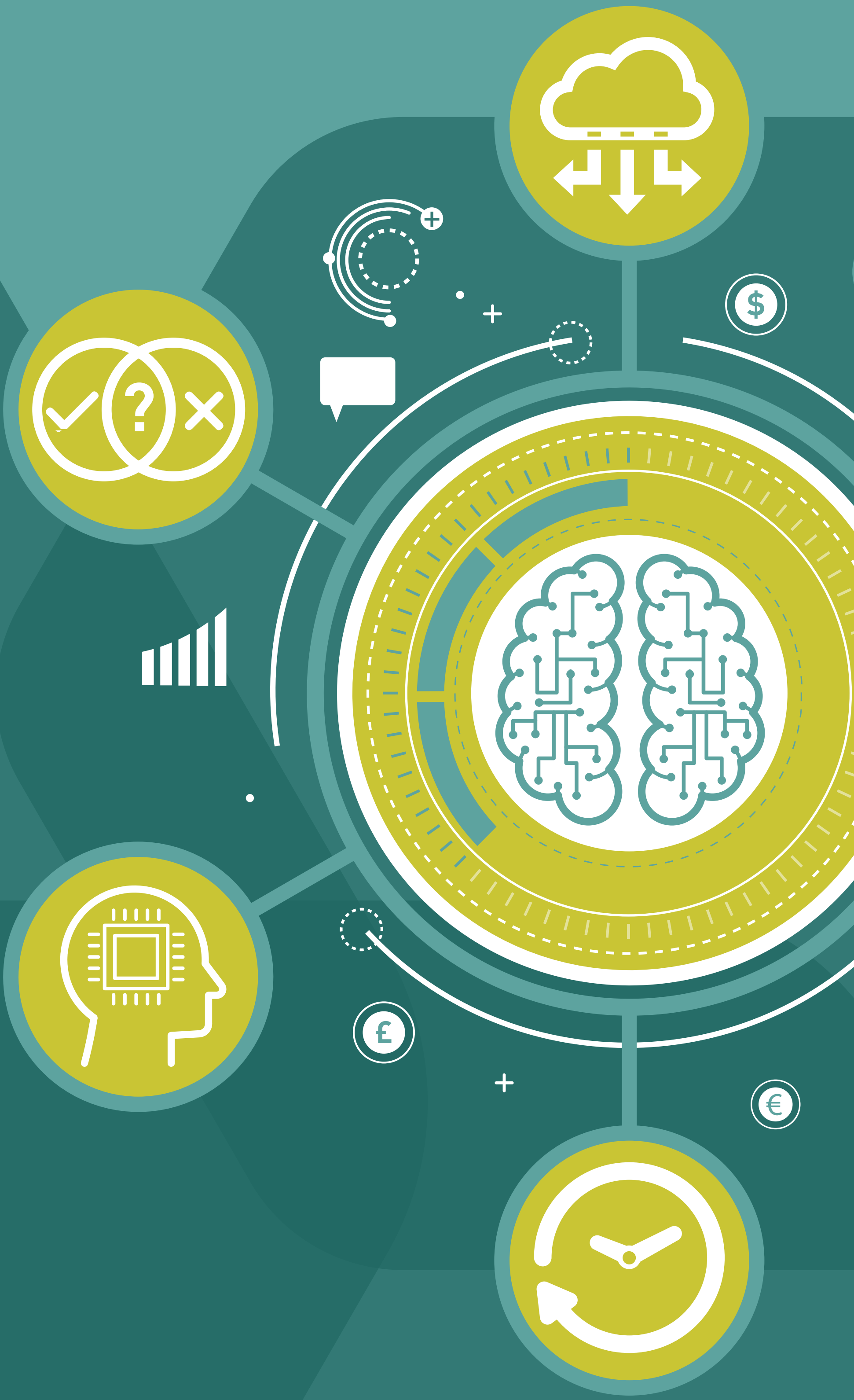
NetGuardians



Digital Banking Fraud:

Best Practice for Technology-Based Prevention

Executive summary

The shift of banking to digital channels is creating a revolution in banking fraud. Until a few years ago, this was the preserve of small-scale criminals attempting to steal relatively modest sums. But today, digital banking fraud is a major international industry in which sophisticated criminal groups employ increasingly sophisticated tools – and frequently collude with corrupt bank staff – to steal very large sums. This in turn has pushed up the liabilities that banks must absorb to cover the losses their customers suffer due to fraud.

As digital channels have multiplied, so have the routes that fraudsters can use. And their options are about to expand again with the implementation of Open Banking and the coming into effect of Europe's second Payment Services Directive (PSD2). This will present a new set of challenges for banks, who will remain liable for losses caused by unauthorized transactions through these new digital channels.

Against that troubling background, this paper examines the variety of ways in which digital banking frauds can take place, detailing seven examples in case studies, and explains the main sources of banks' vulnerability: customers, controls and culture. These vulnerabilities are most effectively addressed by technology-based anti-fraud systems that offer eight critical attributes, which are set out below. These attributes should lie at the heart of any tech-based approach to ensuring effective real-time oversight of the end-to-end digital processes that are now customers' preferred way to access banking services.

Together, they underpin an approach to fraud detection and prevention that analyzes the individual customer's behavior and the overall context in which each transaction takes place in multiple dimensions, and compares the results with that customer's established behavioral profile to flag up anomalies. It is an approach that is drawing increasingly on machine learning and Artificial Intelligence to improve performance and increase sensitivity to the more complex types of fraud that are constantly emerging and spreading from one market to another.

1. The context: fraud on an industrial scale

The digital revolution that is transforming banking is also enabling new forms of banking fraud. The banking transition from branch-based delivery to multi-channel services has opened up a new arena for criminals to operate in. Digital delivery has huge attractions: it is cheaper for banks to provide and it enables more customer-centric strategies, empowering users to access banking services whenever and wherever they want. But it also creates new vulnerabilities. Customers become the weakest links in the chain. Their awareness of online security risks is often poor and they are easily duped into divulging confidential data to criminal groups that can then be used to authenticate fraudulent transactions.

We are witnessing the industrialization of digital banking fraud

Digital channels also have huge attractions for fraudsters. These services create massive volumes of electronic transactions that are processed from end to end automatically. The sheer volume of digital transactions means that traditional manual methods of fraud monitoring and detection have neither the capacity nor the speed to meet the challenge facing banks today.

This explains why we are witnessing the industrialization of digital banking fraud. This is no longer an activity for small-scale criminals attempting to steal relatively modest sums; digital banking fraud is now dominated by organized criminal gangs with access to high-end technology tools and detailed knowledge of banks' internal operations. In 2015, the City of London Police Commissioner warned that the value of thefts from banks through digital channels could already have overtaken that of the international drugs trade. There is even evidence that criminal groups that enjoy state sponsorship or protection are engaged in online banking fraud.

The massive growth in digital fraud is exposing weaknesses in banks' defenses. While banks are investing heavily to provide the real-time digital services that their customers want, they are failing to allocate sufficient resources to keep their services secure. Without adequate anti-fraud systems, many banks struggle to detect dubious transactions before they are completed.

The challenge is particularly acute for smaller banks, where resources are more constrained. Two-factor "strong authentication" of the customer's identity has proved an effective way to reduce digital banking fraud, but it is neither user-friendly nor cheap. Alternative approaches to detecting and preventing digital banking fraud can be both more effective and cover a wider range of circumstances.

CASE STUDY 1

Cyber-heist: the $951m raid on Bangladesh's central bank

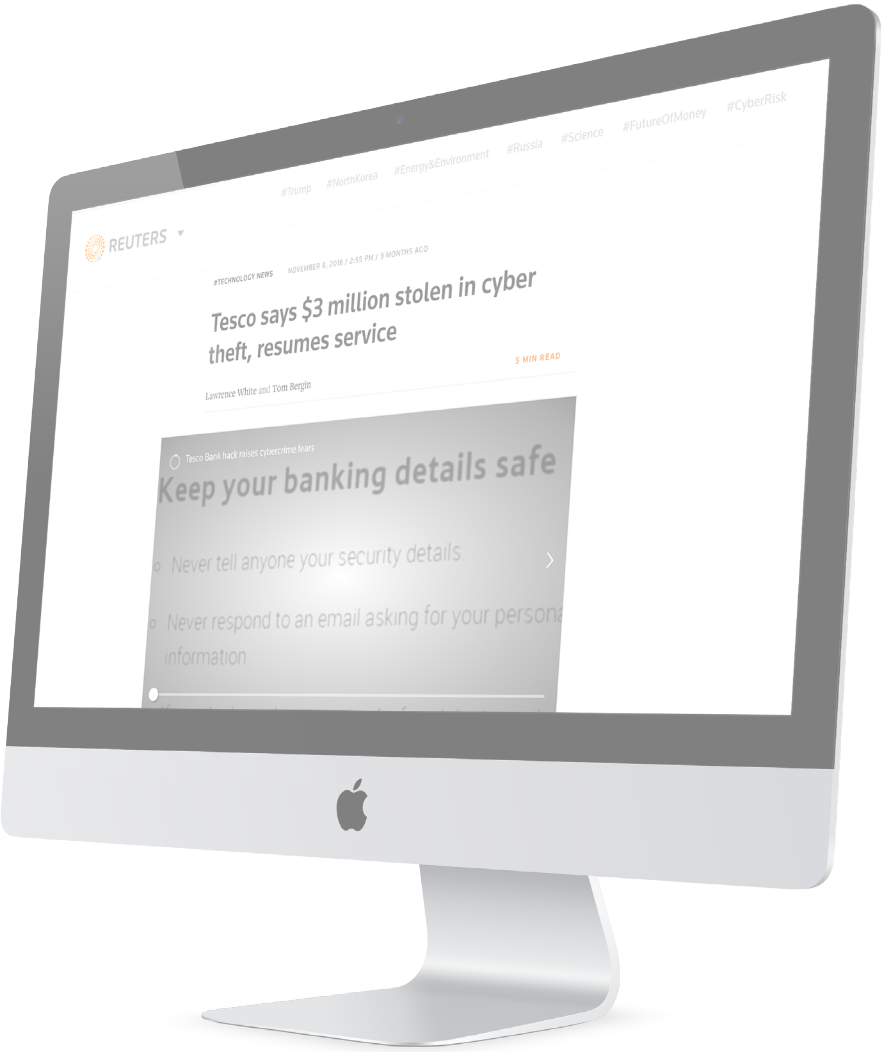
In early 2016, a criminal gang penetrated the security systems of Bangladesh Bank with malware that cloned legitimate transactions. On February 4, the malware sent 35 withdrawal requests through the international SWIFT system to the New York Federal Reserve, where the Bangladeshi central bank had money on deposit. The fraudsters attempted to steal a total of $951m. Thirty of the orders, worth $850m, were blocked by the New York Fed, but the gang succeeded in having $101m transferred to banks in Sri Lanka and the Philippines before their activities were noticed, thanks to a spelling mistake in one of the transfer requests. Subsequently, $20m was recovered from a Sri Lankan bank, but officials were too late to stop the remaining $81m from disappearing. A spokesman for the Federal Reserve of New York said: "The payment instructions in question were fully authenticated by the SWIFT messaging system in accordance with standard authentication protocols."

The gang involved is thought to have consisted of between 20 and 40 members with a range of skills and including financial and banking experts, hackers and software engineers. Had it not been for one slip-up, their audacious attempt to steal almost $1bn might have succeeded – a prospect that has caused huge concern among banks and their institutional customers, which keep large sums on deposit to pay staff and suppliers.

CASE STUDY 2

Tesco Bank suffers UK's first mass account theft

In November 2016, the bank owned by UK supermarket group Tesco suffered a huge online security breach in which a total of £2.5m was removed from 20,000 of its 136,000 current accounts and suspicious activity was discovered on a further 20,000. The robbery happened over a weekend, while bank staff were absent, and there has been no official explanation of exactly how the thefts were executed. However, experts suggested that hackers had identified a weakness in the Tesco Bank website and exploited it to steal thousands of customers' account details that were then used to make online purchases. On discovering the fraud, Tesco temporarily blocked online payments by its current-account customers while continuing to allow them to use cards for cash withdrawals, chip and pin, and bill payments.



#TECHNOLOGY NEWS NOVEMBER 8, 2016 / 2:55 PM / 9 MONTHS AGO

Tesco says $3 million stolen in cyber theft, resumes service

5 MIN READ

Lawrence White and Tom Bergin

Tesco Bank hack raises cybercrime fears

Keep your banking details safe

- Never tell anyone your security details.
- Never respond to an email asking for your persona information.

2. The looming challenges of Open Banking

Digital technologies are transforming the way people access banking services, as well as turning digital banking fraud into a fast-growing global industry. But huge regulatory changes are also approaching that will create new potential threats to bank security and give banks wider liabilities for fraudulent transactions on their customers' accounts.

From early 2018, the European Union's second Payment Services Directive (PSD2) will come into force, alongside the Open Banking competition remedies imposed in parallel by the UK's Competition and Markets Authority on the country's nine largest banks. These two measures will oblige banks to facilitate the sharing of highly-confidential data with third-party services providers via Open Application Program Interfaces (APIs). For banks that have historically concentrated above all on protecting their customers' data and ensuring confidentiality, the PSD2/Open Banking rules represent a significant challenge; provided customers give their consent, banks must enable third parties to access the customer's transaction history and to initiate direct payments from their accounts to pay for goods and services.

> **Huge regulatory changes are approaching that will create new potential threats to bank security**

This should result in a wide range of new and innovative banking and financial services that will deliver great value to customers. But the arrival of Open Banking will also create additional opportunities for digital banking fraud at a time when banks are already locked in an escalating arms race against digital fraudsters with access to ever more sophisticated tools.

Under the PSD2/Open Banking regime, banks will be liable for unauthorized transactions that take place on customers' accounts through Open APIs. They will therefore have to verify that any apparent consent from a customer for their data to be shared or for a payment to be initiated is genuine; failure to do so will create a liability under PSD2 for any losses the customer suffers.

However, the security challenge for banks will change fundamentally because in an Open Banking market, customers will not necessarily have to log into their bank's digital services to carry out transactions; instead they will be able to give their consent to a third-party provider that will then initiate a payment from their account via an API. This will reduce the amount of data that the bank can use to judge whether any individual transaction is legitimate or not and will therefore require banks to look at profiles/behaviors of customers at individual level and to fast-track the development of real-time anti-fraud systems that can detect and prevent Open Banking fraud.

3. The risks: how and where cyber-fraud happens

There are numerous ways for fraudsters to penetrate digital banking systems and carry out thefts, often thanks to poor security awareness among banking customers, who write down passwords or can be tricked fairly easily into divulging them.

So-called phishing scams that use links in emails to direct customers to fake online banking webpages are well documented. In June 2013, three men were jailed in the UK for a total of 20 years after police uncovered a phishing scam that targeted people in 14 countries and involved 2,600 fake webpages. After their arrest, the Metropolitan Police's Central e-Crime Unit located servers containing details of 30,000 bank customers, including 12,500 in the UK, and 70 million customer email addresses. They produced evidence at the men's trial that their arrest had prevented the theft of up to £59m from UK bank customers alone.

Phone-based frauds, where criminals pose as bank staff to persuade victims to divulge their login details, are also widespread, although fraudsters are also exploiting a growing range of channels to steal confidential information.

CASE STUDY 3

Android malware installs fake apps on smartphones

In June 2017, security specialists at FireEye reported that they had identified malware that installs fake versions of eight popular apps including Facebook, WhatsApp, Uber, Google Play and Viber on victims' smartphones. They are sent a text message saying: "We have not been able to deliver your order. Please check your shipping information here", followed by a link. Once the victim clicks the link, it installs the malware, which waits for the user to open one of the targeted apps. The malware then overlays a fake interface on top of the legitimate app and attempts to trick victims into divulging their online banking information. The phishing texts were first seen in Denmark, where 130,000 victims were tricked into clicking the link. The malware is thought to have spread to the UK, Germany, Luxembourg, Spain, Sweden, Norway, the Netherlands, Italy, Greece and Turkey.

Many phishing-type scams now involve significant elements of 'social engineering', in which the criminals use information gleaned from their victims' social media profile, pose as officials to phone victims and check their personal details, and even intercept their mail to build a profile of the victim that will allow the fraudster to impersonate them. The information gained may be used to create lists of possible passwords that can be used in attempts to crack their online accounts. However, it can also be used to steal the victim's identity and make fraudulent applications for financial products. Cifas, the UK fraud prevention service, states that a record 173,000 identity frauds were reported in the UK in 2016 and that nine out of 10 fraudulent applications for bank accounts and other financial products were made online.

173,000

identity frauds were reported in the UK in 2016

CASE STUDY 4

Stolen dongle used in attempt to crack 'strong authentication'

In one recent Swiss case involving a corporate client of a bank, 10 employees had the authority to issue payments in the name of the corporation but only three normally did so. One of the remaining seven staff had his dongle stolen but since he was not among the group that normally issued payments he did not immediately notice the theft. The thief waited eight months before attempting to initiate a transaction using the stolen dongle, but his attempt raised a flag and was blocked. However, the case highlights the need to check whether the person attempting to issue a payment is one of the normal users of the system or part of a wider group that has the authority to do so.

Rogue software is another favorite tool of fraudsters, who infect customers' devices with worms and malware that recognize when they are signing into online banking services and log their keystrokes, enabling the criminals to steal their passwords. Both malware and physical hijacking of the line can also be used to initiate a fake transaction during an online banking session that the victim might re-authenticate by mistake among a succession of legitimate transactions.

Although the customer is often the weak link in online banking security, internal fraud and collusion between bank staff and external criminals is extremely common. KPMG estimates[1] that about one-in-three frauds involves collusion between insiders and criminals outside the organization.

Criminal gangs are experienced in identifying employees who can be compromised, either because of grievances against their employer over pay or promotion, or because they have large personal liabilities. Once recruited, these internal sources can feed confidential data to criminal gangs or disable system logs so that activity can go unrecorded. Collusion often focuses on larger-scale frauds involving institutional accounts, since the sums available from personal accounts are not usually large enough to warrant the risk and effort involved in recruiting an inside accomplice.

[1] Global Profiles of the Fraudster', KPMG, May 2016, see: https://assets.kpmg.com/content/dam/kpmg/pdf/2016/05/profiles-of-the-fraudster.pdf

Poor enforcement of internal controls is often a key factor in the success of frauds involving internal collusion. If oversight is compromised, for example the four-eyes principle, staff working with the fraudsters are able to verify or reverse a transaction that allows a theft to proceed.

CASE STUDY 5

Poor security at software supplier opens the door to fraudsters

In one recent East African case cited by fraud specialist Gilbert Nyandeje, chief operating officer of Enovise, a software developer at the company hired to build a mobile banking app left a "back door" in the source code that was not detected before the app went live. Once implemented, the back door created an outgoing, or reverse, connection from the bank's systems that criminals could use to access customer accounts, stealing a total of more than $50,000 before the flaw was detected. This method of breaching the bank's security succeeded because while internal firewalls prevent outsiders from getting into the system, they do not necessarily block outgoing connections.

4. Know your weaknesses: the three Cs – customers, controls and culture

To secure themselves against fraud via digital channels, banks need to identify and address the areas where they are vulnerable. These include ensuring that basic IT security precautions are in place, applying appropriate internal controls rigorously, and telling their customers how to bank safely online, choose strong passwords and avoid being duped.

The major problem that most banks face is that their investment in infrastructure security has failed to keep pace with their efforts to provide the digital services that customers now expect. As a result, many frauds are being detected by customers rather than the banks themselves, undermining trust in bank brands. Complaints and tip-offs are the main way in which frauds are detected, accounting for a quarter of all cases. Particular vulnerabilities of banks include:

- Many smaller institutions do not have dedicated fraud teams.

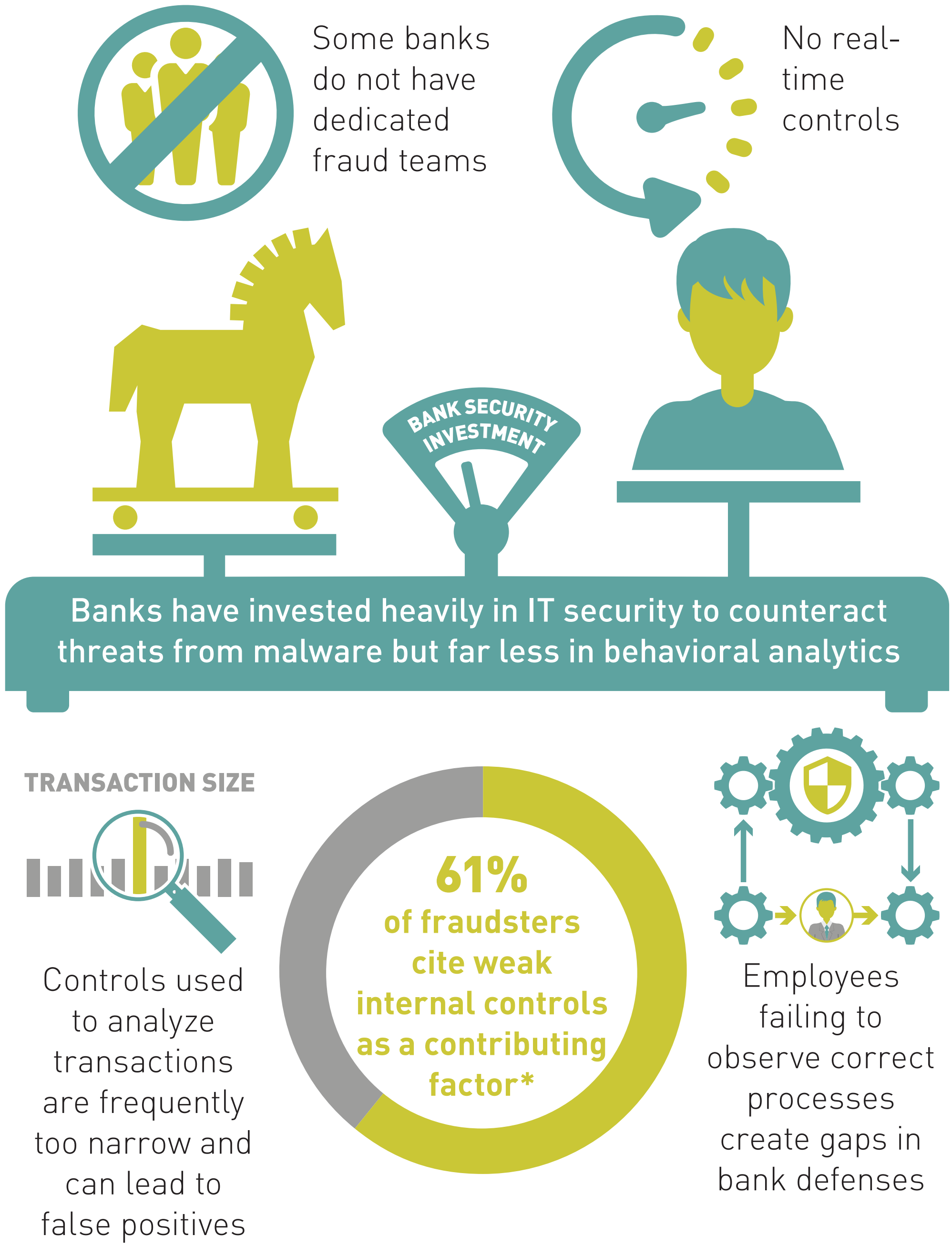
- Banks have invested heavily in IT security to counteract threats from malware such as viruses, worms, trojans and so on, but have invested far less in areas such as behavioral analytics that can help them detect unusual patterns of account use that could indicate criminal activity.

- Controls are frequently inadequate because they are not enforced in real time and are therefore too slow to block digital transactions that are processed automatically.

- Controls used to analyze transactions are frequently too narrow, identifying suspect transactions by their size alone and ignoring the broader context. This produces too many false positives, wasting the time of compliance staff and inconveniencing customers.

- More generally, too many banks have a weak control culture, where employees do not observe the correct processes and therefore create gaps in the bank's defenses that can allow fraud to slip through. According to KPMG's report *Global Profiles of* *the Fraudster* (May 2016), in 61 percent of cases weak internal controls were a contributing factor, up from 54 percent in the firm's previous report from 2013. In Europe, 72 percent of fraudsters told KPMG that weak controls presented the opportunity they were looking for.

Particular vulnerabilities of banks include:



Some banks do not have dedicated fraud teams

No real-time controls

Banks have invested heavily in IT security to counteract threats from malware but far less in behavioral analytics

Controls used to analyze transactions are frequently too narrow and can lead to false positives

61% of fraudsters cite weak internal controls as a contributing factor*

Employees failing to observe correct processes create gaps in bank defenses

*KPMG's report Global Profiles of the Fraudster (May 2016)

CASE STUDY 6

Poor controls allow collusion on mobile fraud

Nyandeje points to another East African case where poor processes allowed a corrupt employee to gain access to the account opening forms that customers filled in and left at their bank branch. The details of the newly-created account were passed to an outside accomplice who then applied to set up mobile banking, giving a fraudulent mobile number that was connected on the bank's systems to the legitimate account. With the ability to authenticate fraudulent mobile transactions on numerous customer accounts, the gang went on to steal large sums.

To address their major areas of weakness, banks need to focus on robust oversight of employee access to bank systems. If members of staff have access to both front-office and back-office systems, they can obtain sensitive customer information that could be passed to criminals outside the bank, and also approve the fraudulent transactions as they pass through the system. Each employee's access privileges must be regularly reviewed and amended as appropriate.

There are also issues with the established culture in many banks, which have a long-standing preference for developing bespoke technology systems internally rather than adopting existing, proven technology from external providers. This preference for proprietary systems is leaving banks increasingly vulnerable: relying on technology developed in-house increases the risk that they will be overtaken by the growing sophistication of the technology available to criminal gangs. In some markets, such as the UK, banks are more advanced in working with fintech companies, but generally there is a need for a change in banking culture to promote more openness to external innovations in many areas, including advanced fraud-detection techniques.

5. The case for technology: eight reasons why it wins

Improving technology tools are enabling criminal gangs to execute more complex frauds; a technology-based strategy is the only practical response if banks are to succeed in safeguarding their brand reputation and customer trust. Advanced anti-fraud systems offer eight critical strengths in banks' fight against fraud.

Timeliness: technology automates anti-fraud systems and can therefore detect possible instances of fraud in real time as they happen. This allows suspicious transactions to be blocked as they pass through the bank's systems and staff alerted to check and validate them before they are cleared. Controls designed to combat fraud executed through non-digital channels do not work effectively against digital banking frauds because they cannot be executed in real time.

As volumes of digital banking transactions grow, technology provides the only scalable way to respond

Comprehensiveness: a technology-based approach allows the bank to monitor every transaction in its system – an impossible feat for humans. As the volumes of digital banking transactions continue to grow, technology provides the only scalable way to respond.

Risk sensitivity: even genuine customers sometimes carry out transactions that are outside their normal pattern of behavior. Advanced fraud detection systems allow the bank to evaluate the risk of any transaction using a range of variables, helping them to avoid blocking legitimate transactions and identify others that are apparently genuine but have suspect characteristics.

Focus on the individual customer: digital banking fraud depends on the criminal's ability to pose as the account holder, using stolen identity data, and thereby to convince the bank's security checks that the transactions are legitimate. To combat this threat effectively, banks need to be able to judge when an imposter is using genuine identity data to carry out fraudulent transactions.

Therefore, banks must understand each customer's established patterns of behavior so that every transaction makes sense when compared to his or her profile. Technology offers the only effective method of monitoring transactions and detecting anomalies in this way.

360-degree surveillance: banks face the threat of fraud from every direction. Collusion between criminal gangs and bank staff is a recurring problem and is thought to feature in up to four-fifths of all fraud cases. Tech-based monitoring enables banks to monitor both customers and their own staff through a single system and dashboard, helping to defend the bank against more complex frauds that involve both internal and external actors.

Efficiency: expert staff are an expensive and scarce resource that must be deployed efficiently. With advanced technology systems as their first line of defense, banks are able to make better use of their employees' time and skills, focusing them on the investigation and verification of suspect cases flagged by the anti-fraud system.

Record-keeping: regulators demand comprehensive records to prove that banks have effective measures in place to combat fraud and can demonstrate that they are investigating cases thoroughly. Automated fraud detection systems produce full audit trails and facilitate proper record-keeping, helping the bank comply with regulatory requirements.

Ability to learn: new technologies based on machine learning enable anti-fraud systems to become intelligent. This helps to identify new risks before they lead to losses, and to anticipate new types of fraud.

Eight reasons why technology wins

Timeliness

Automated anti-fraud systems can detect possible instances of fraud in real time and block them before they happen

Comprehensiveness

A technology-based approach allows a bank to monitor every transaction in its system – an impossible feat for humans

Risk sensitivity

Banks avoid blocking legitimate transactions and identify others that seem genuine but have suspect characteristics

Focus on individual customer

Banks must understand each customer's behavior patterns so every transaction makes sense when compared to their profile

360-degree surveillance

A tech-based approach enables banks to monitor both customers and their own staff through a single system

Efficiency

Expert staff are freed up to focus on the investigation and verification of suspect cases flagged by the system

Record-keeping

Automated fraud-detection systems facilitate record-keeping, helping banks comply with regulatory requirements

Ability to learn

Intelligent systems make it possible to identify new risks before they lead to losses and anticipate new types of fraud

NetGuardians

6. Outlines for a tech-led solution: behavioral data analytics holds the key

Using the eight key strengths outlined above, it is possible to set out an effective solution to digital banking fraud based on technology tools available today.

This solution is based on a risk model that incorporates a detailed behavioral profile of each customer, coupled with a range of other variables, to create a template against which every transaction that takes place on their accounts can be compared and evaluated automatically. These risk models are increasingly using machine-learning techniques to improve their sensitivity and ability to differentiate between legitimate transactions and frauds.

The system takes every customer's transaction history and builds a detailed profile based on their digital banking behavior – where and when they normally transact, their normal range of counterparties, the ways they typically access the bank's systems and the usual size of transactions. This technique is applied both to individual customers and to institutional accounts

CASE STUDY 7

How unusual activity signals a fraud

A recent case in Switzerland is a perfect illustration of how behavioral analytics looking for suspicious activity could stop fraud. In March, a Swiss company's bank accounts were hacked and SFr1.2m fraudulently transferred to an account in Kyrgyzstan. Although four Swiss banks were involved, only one blocked the transfer after spotting a spelling mistake. The chairman of the company targeted by the attack believes the others should have noted something was awry and done the same; the destination account belonged to an individual who had never received funds from his company before – this alone should have been enough to raise an alert.

that have multiple authorized users. The profile that the system creates becomes part of the template against which every future digital banking transaction is correlated to assess whether it matches the customer's established patterns of behavior.

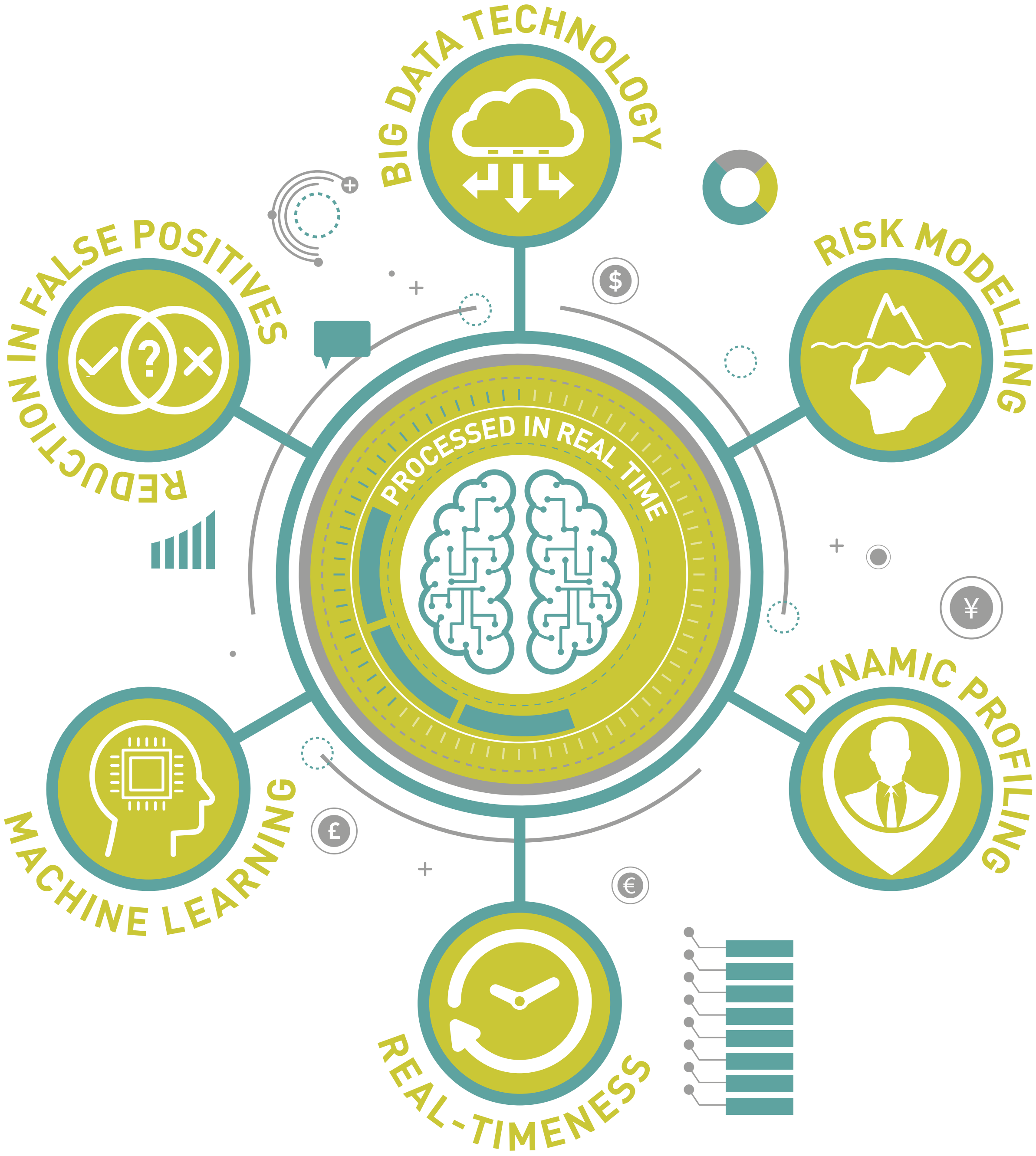
This behavioral information is augmented by a wide range of contextual information covering variables such as the customer's geolocation, time of day, week and month, the device, web browser and type of webpage that is being viewed, the type of account involved (individual or institutional, for example), the domestic or international destination of any payments, whether the payee is new or previously known, and so on. When individual transactions are assessed against the risk model, it computes the probability that the transaction is fraudulent based on the specific conditions in which it takes place and the extent to which it differs from the recognized pattern of behavior connected with that account.

Importantly, where some anti-fraud systems analyze transactions by size alone, flagging everything above a certain value, advanced systems draw on a wider range of contextual information to focus the search, reducing the number of false positives.

The effectiveness of technology-based anti-fraud systems depends crucially on their ability to operate in real time, so that suspect activity can be flagged immediately and transactions blocked. Most anti-fraud systems that employ advanced analytics, incorporating detailed user profiles, cannot operate in real time and risk failing to detect fraudulent activity quickly enough to prevent losses. However, the most advanced anti-fraud systems employ Big Data technology, allowing them to apply the advanced analytical techniques to huge volumes of transactions in real time.

In common with every type of security measure, transaction-monitoring systems must balance the need to provide more effective fraud prevention against the inconvenience caused to customers when legitimate transactions are blocked. Thanks to the wide range of contextual information incorporated into their risk models and the increased utilization of machine learning techniques, advanced anti-fraud systems can be tuned to reflect the requirements of individual banks and the range of institutional and personal customers they serve. This helps to reduce the proportion of false positives that the system flags up, while ensuring that it remains sensitive enough to capture a high proportion of frauds.

Outlines for a tech-led solution for digital banking fraud prevention



NetGuardians

Conclusion

The 'arms race' between criminals and security specialists is entering a new phase. Cyber-fraud began with a few individual hackers trying to steal relatively modest sums; it is now a global illicit industry involving gangs of skilled criminals with inside knowledge of the financial system and access to very sophisticated technology tools. As a result, patterns of fraud are becoming more complex, they involve more people and they frequently depend on collusion between criminal gangs and people inside the bank. The more sophisticated cyber-fraud becomes, the higher the risk that it will fool the monitoring systems that banks rely on to catch fraudsters.

The most advanced anti-fraud systems on the market are using Big Data technology to apply advanced analytical models in real-time, giving banks the capacity to prevent fraud as it occurs.

At the same time, regulation is also creating new areas of potential vulnerability for banks. Moves in several developed markets towards Open Banking, thanks to measures such as the EU's second Payment Services Directive (PSD2), will oblige banks to give direct access to their customers' personal banking data via APIs. This will give alternative providers better insights into potential customers' financial situations, enabling them to offer more relevant and competitive services. However, Open Banking will also create new opportunities for customer data to fall into the wrong hands. The risk to bank security is far from negligible.

It is clear, therefore, that fraud detection tools must keep improving to match the developing threat from professional fraud gangs and the new areas of vulnerability that will develop as the digitalization of banking evolves.

The most advanced anti-fraud systems on the market today are using Big Data technology to apply advanced analytical models in real time, giving banks the capacity to identify and block suspicious activity as it occurs. What's more, advanced computing techniques are creating a new generation of tools to combat fraud. Machine learning is already becoming a key tool in advanced anti-fraud systems and its role is certain to grow significantly. New generations of risk modeling, using machine-learning systems that have been trained to spot fraudulent transactions amid vast volumes of banking data, are starting to replace the statistical, probability-based approach that has been used up to now. At the same time, computer scientists are creating anti-fraud systems that are more sensitive to the complex patterns of fraud and collusion that are a feature of professionally-executed cyber-frauds.

Better-tuned and more sensitive systems, in turn, will allow banks to strike a better balance between detecting fraud and allowing customers to carry out their transactions unhindered. Improving technology tools and the introduction of innovative techniques based on machine learning are giving banks access to sophisticated anti-fraud systems that are more effective, more efficient and less intrusive for customers. Those banks that implement them can expect lower percentages of false positives, lower losses to fraud, improved customer service and less time wasted on compliance and verification to investigate false positives.

All of these ultimately contribute to strengthening the most important asset that banks possess: the customers' trust in their brand.

NetGuardians

For further information on Digital Banking Fraud Prevention, please contact:

NetGuardians
info@netguardians.ch

Rue Galilée 6
1400 Yverdon-les-Bains
Switzerland
T +41 24 425 97 60
F +41 24 425 97 65

www.netguardians.ch

ABOUT NETGUARDIANS

NetGuardians is a leading FinTech company recognized for its unique approach to fraud and risk assurance solutions. Their software leverages Big Data to correlate and analyze behaviors across the entire bank system – not just at the transaction level. With predefined controls, NetGuardians enables banks to address anti-fraud or regulatory requirements. Headquartered in Switzerland, NetGuardians has offices in Kenya, Singapore, and Poland.