TEMENOS
The software specialist for banking and finance

NetGuardians

A-Z of Banking Fraud

The What, Why and How

"Banking fraud cost an estimated $64bn in 2014. 70% WAS INTERNAL. Most remains undetected"

Association of Certified Fraud Examiners, Report to the Nations

Welcome to the Temenos and NetGuardians A-Z of Banking Fraud – a comprehensive e-book outlining the what, why and how of fraud; exploring the size of the issue, who commits it and, most importantly, what can be done.

Fraud is big business, costing the banking industry $67 billion per annum, according to the Association of Certified Fraud Examiners. It's a problem no one can afford to ignore as firms struggle to recover from the global financial crisis and the world's major economies teeter on the edge of recession. Most worrying of all, its incidence is escalating.

In 2014, the US State of Cyber Crime Survey showed a year-on-year increase of 141 per cent in the number of financial institutions reporting losses of between $10 million and $19.9 million. In reality that figure is likely to be higher because many cases never get referred to external authorities.

The most alarming statistic relates to insider fraud: in 70 per cent of cases, the crime was perpetrated by a bank employee. Those with the highest levels of access to IT systems, such as systems and database administrators, are well placed to commit or facilitate it – and erase all evidence of their actions.

Fraudulent behaviour can be very difficult to detect amid the large number of bona fide transactions that a bank carries out each day. New channels such as online banking, mobile apps and social networks only add to the complexity of the task, hampered by legacy systems that make IT security hard to police.

But cutting-edge technologies such as continuous auditing, big data analysis and profiling are available today. Real time processing detects fraudulent activities before it even happens, and delivers information in a form that won't require data scientists to interpret it. Risk, Audit and Compliance are able to see more than the tip of the iceberg.

Such knowledge is power. To put bankers on the right track, Temenos and NetGuardians have teamed up to compile this indispensable A-Z guide. We hope it's thought provoking – and not too worrying – that it stimulates discussion and provides reassurance for the future…

Yours truly,

Ben Robinson, Temenos

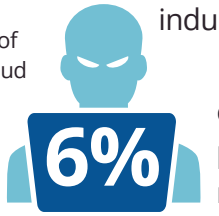
Joel Winteregg, NetGuardians

Quantum of fraud

The scale of fraud committed against banks is hard to determine precisely because many cases go unreported. However, information from within the industry suggests that:

Total value of banking fraud in 2014
(Source: Association of Certified Fraud Examiners)

70%
of fraud is committed by industry insiders ie employees



of banks' global pre-tax profits were lost as a result of criminal activity*

Three-quarters
of financial services companies experienced at least one incidence of fraud in 2012-13

On average, these business incurred losses equivalent to **1.5%** of their revenues
(Source: Economist Intelligence Unit)

141%
increase in the number of financial firms reporting losses of between **$10m** and **$19.9m**
(Source: 2014 US State of Cybercrime Survey)

30% of financial services companies have been affected by data theft – individually the most common form of fraud within the industry

IT complexity cited as the top risk factor that organisations face

Fear of **bad publicity** is the most frequently cited reason why cases of fraud are not referred to criminal prosecutors. Plus the cost and time necessary to carry out an investigation

*Value of banking fraud calculated as a percentage of total pre-tax profits of top 1,000 banks in 2014, addording to data from The Banker

A Access

ACCESS is the most important ingredient in any bank fraud and more than anything else this means access to the IT systems that run the bank's day-to-day operations and enable its customers to manage their accounts. Gaining uncontrolled access to the bank's IT systems enables a fraudster to steal or alter sensitive information, execute illicit transactions and remove evidence of their activities. It is, of course, possible for fraudsters to break into a bank's IT systems from outside if they are able to exploit weaknesses in its security. However, in practice it is much more likely that a bank will experience fraud that originates within the organisation due to the high level of access to sensitive data that must be granted to thousands of staff in order for them to do their jobs.

- Many staff are able to see sensitive customer information in the course of their work, but staff in certain crucial roles will have greater user privileges than most of their colleague. They will therefore have a much higher degree of access to the system and the ability to change and update it without necessarily attracting any scrutiny. In particular, the roles of IT systems administrators and database administrators both require that they have very high levels of access to the bank's critical systems. The activities of systems and database administrators should attract special attention within a bank's security monitoring and it is vital that staff such as these with high user privileges are not able to bypass audit trails and operate "below the radar".

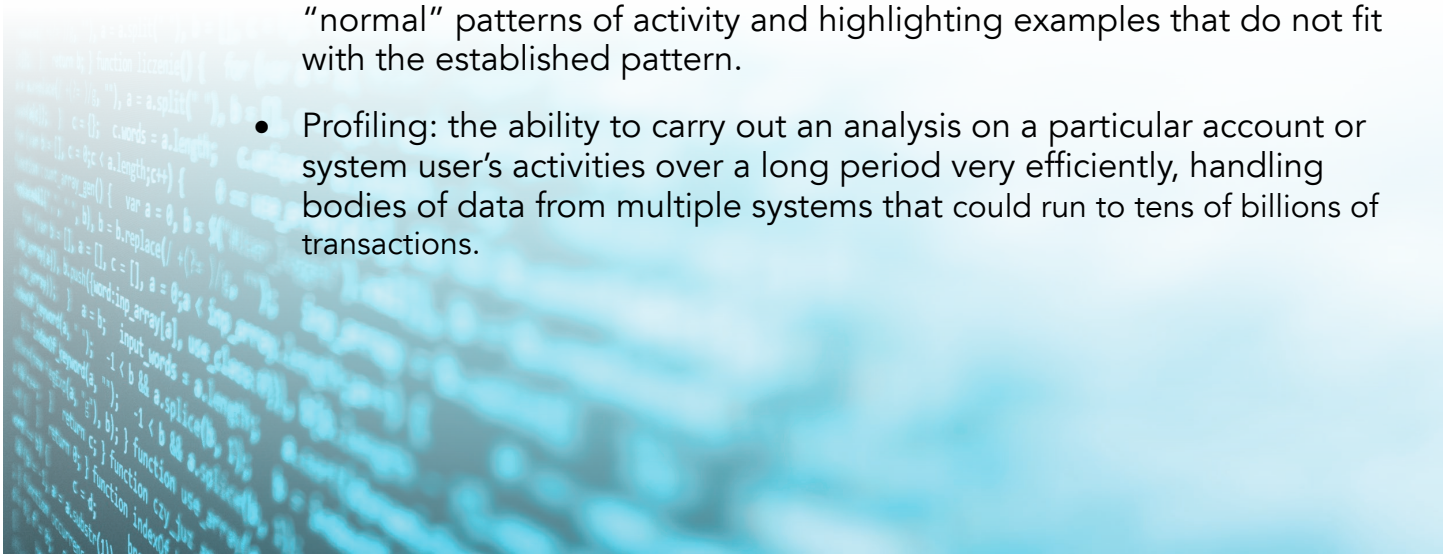
B BIG DATA

BIG DATA is shorthand for the ability of modern computer systems to bring together very large volumes of data from multiple sources and analyse them in order to unlock valuable insights – in this case signals suggesting that fraudulent activity is taking place. As computing power has both multiplied and become cheaper over recent years, so systems have emerged that are able to analyse very large bodies of data in close to real-time, greatly increasing the speed at which valuable information and insights become available.

In the case of banks, big data analytics can be used to bring together, interpret and detect meaningful correlations in data from different IT systems within the bank that are not connected and do not normally interact with each other, ranging from mobile, e-banking and transactional systems to core banking, CRM and physical access data. For example, by comparing information in the bank's transactional systems with data on physical access to the premises by staff members, one can detect the use of a staff member's log-in when they are not present in the building, within minutes of a breach occurring.

There are three main ways in which big data analytics are used to look for and detect bank fraud:

- Detecting breaches of the bank's controls: searching for a precise and well-defined pattern of activity on the system that contravenes the bank's system.
- Carrying out analysis to detect abnormal behaviour that may not in itself breach any control. This involves the system learning to recognise "normal" patterns of activity and highlighting examples that do not fit with the established pattern.
- Profiling: the ability to carry out an analysis on a particular account or system user's activities over a long period very efficiently, handling bodies of data from multiple systems that could run to tens of billions of transactions.



Big data, profiling and how they can help

This is the ability of modern computer systems to bring together very large volumes of data from multiple sources and analyse them to unlock valuable insights – such as signals that fraudulent activity is taking place.

FOR EXAMPLE

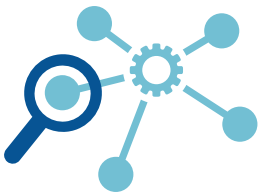
By comparing information in a bank's transactional systems with data on access to the premises, it's possible to detect the use of a staff log-in when they are not present in the building – within minutes of a breach occurring

There are three ways in which big data analytics can look for fraud:

1. Searching for precise patterns of activity that breach the bank's system of controls

2. Detecting abnormal behaviour that may not itself breach any controls but enables the system to learn "normal" patterns of activity and highlight examples that do not fit

3. Profiling a particular account or system user's activities over a long period, which could run to tens of billions of transactions



In a **customer** context, activities outside the normal profile might include an ATM withdrawal in a different country, a transaction of unusual size or one that takes place at an unexpected time of day

In an **investment banking** context, profiling the net positions and trading activity of a group of traders might enable their employer to discover patterns that differ from colleagues in the same team

Coming soon: predictive analysis of user behaviour and transaction patterns will give early warning of suspect activities

C Complexity

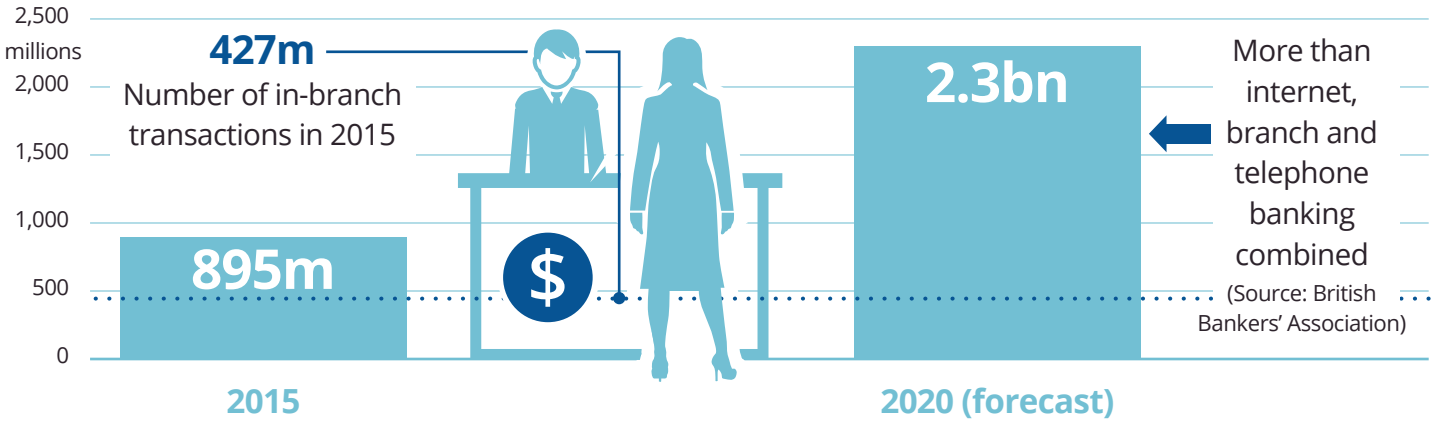
COMPLEXITY represents probably the most important source of vulnerability that banks suffer in attempting to detect and prevent fraud. As banking has become increasingly dependent on technology – and in the absence of a countervailing strategy – the systems that banks depend on to deliver their services have multiplied and grown much more complex. The effect of this process of increasing complexity has been to create more opportunities for fraudsters to gain access to critical systems, while at the same time making it harder for banks to have a clear overview of all the activity taking place on their systems.

Complexity in bank systems can be seen in the growing number of channels through which banks now deliver their services, including websites and online banking platforms, mobile apps and social networks. All these channels represent a new set of opportunities for fraudsters to gain access to the bank's information system. Banks' IT has become more complex as new information systems are implemented on top of older systems, building up layers of technology that do not necessarily link together and so make it much more difficult to gain a unified view of operations. As mainframes have given way to network computing, critical systems have also become more distributed: today even a relatively small institution will have multiple databases running on different servers that are accessible to a large number of staff. Complex and highly distributed IT systems such as these are difficult to police and present more opportunities for fraudsters to gain entry. Modernising the legacy systems on which many banks still depend can also increase their ability to detect fraud, a factor that is often overlooked.

Technology and complexity

From online banking platforms to mobile apps and social networks, a growing number of new channels makes it harder for banks to have a clear overview of all the activity taking place on their systems.

Number of times British consumers will use mobile devices to check their current accounts



RISK

IT security becomes more complex as new information systems are implemented on top of older ones. This builds up layers of technology that do not necessarily link together well and are hard to police

RISK

Even a relatively small institution will have multiple databases running on different servers that are accessible to a large number of staff – and people are the weakest link

BENEFIT

Because mobile banking is largely customer driven and fully automated, its growth should help to reduce banks' exposure to fraud – particularly that carried out by insiders...

... BUT

Straight through processing, where there is no human involvement in a transaction, puts huge emphasis on the effectiveness of internal control systems

D Data theft

Although most people might think of fraud as the act of carrying out illicit transactions, DATA THEFT plays a very important role in facilitating the crime and is an area of great concern for banks and their regulators. Banks hold very large quantities of sensitive data on their customers and confidentiality is a basic expectation of any bank customer. Theft of confidential data is therefore damaging to a bank's reputation, even if there is no direct financial loss as a consequence. Data thefts can occur as a result of outsiders gaining access to information systems, but are just as likely to result from internal breaches carried out by staff with high levels of access, such as database and systems administrators. There is a thriving black market on the internet in stolen customer information, including online bank and credit card details.

In the most famous recent example of a large data theft, computer specialist Herve Falciani stole the details of 24,000 private banking clients from a branch in Geneva while working on an IT project in 2007. He subsequently passed the stolen files to French tax authorities. In this instance, the data theft did not facilitate fraud against the bank or its customers, although it did produce a strong response from the bank's regulators because of the serious breach of client confidentiality that resulted. In recent years financial regulators have stepped up pressure on banks to improve their controls around data security and to provide greater protection of clients' confidentiality. The Swiss regulator, FINMA, has published new rules on the security of client identifying data.

E External fraud

EXTERNAL FRAUD, in which an outsider manages to penetrate the bank's data security and access sensitive information or carry out fraudulent transactions, can be achieved in a variety of ways. Poor password security, for example, might allow a fraudster to gain access to the bank's information systems without the need for sophisticated computer hacking. However, much of the fraud carried out by outsiders in fact depends on help and collusion from employees, who may have been paid relatively small sums of money to facilitate the crime.

For example, as mobile banking has grown in popularity, mobile phones have become an accepted way for banks to authenticate a user's identity without them being present. This opens up a new potential vulnerability in the bank's controls that can easily be exploited by an external fraudster colluding with a bank employee who has access to the bank's customer relationship management database. In order to carry out the fraud, the employee temporarily changes a customer's mobile phone number on the bank's database to the number the fraudster will use. The external accomplice then calls the bank's helpline and resets the customer's account password, using the mobile number now showing on the bank's database to validate his or her identity. Once the account has been raided, the bank employee changes the mobile number shown on the database back to the correct one and the fraud is complete.

This again shows how easily a database administrator can make changes to a customer's information without creating an alert suggesting that controls have been breached.

Outside chance

External fraud, in which an outsider manages to penetrate the bank's data security and access sensitive information or carry out fraudulent transactions, can be achieved in a variety of ways.

Poor password security might allow a fraudster to gain access to the bank's IT systems without the need for sophisticated computer hacking

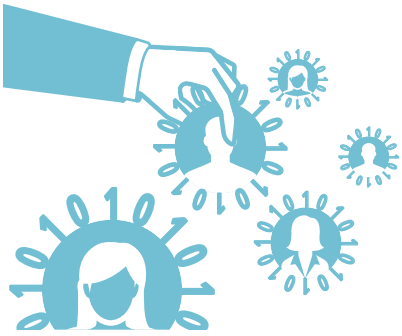
Outsiders usually rely on help and collusion from bank employees – who may have been paid relatively small sums of money to facilitate the crime

Mobile phones are a means to verify a customer's identity without them being present, but leave banks vulnerable to simple frauds.

Here's how it works: an "insider" changes a customer's mobile number on the CRM database to the one the fraudster will use...

The external accomplice then calls the bank's helpline and resets the customer's password...

Once the account has been raided, the information on the database is changed back.



There is a thriving black market in stolen customer information, including online bank and credit card details

Theft of confidential data is damaging to a bank's reputation, even if there is no direct financial loss as a consequence

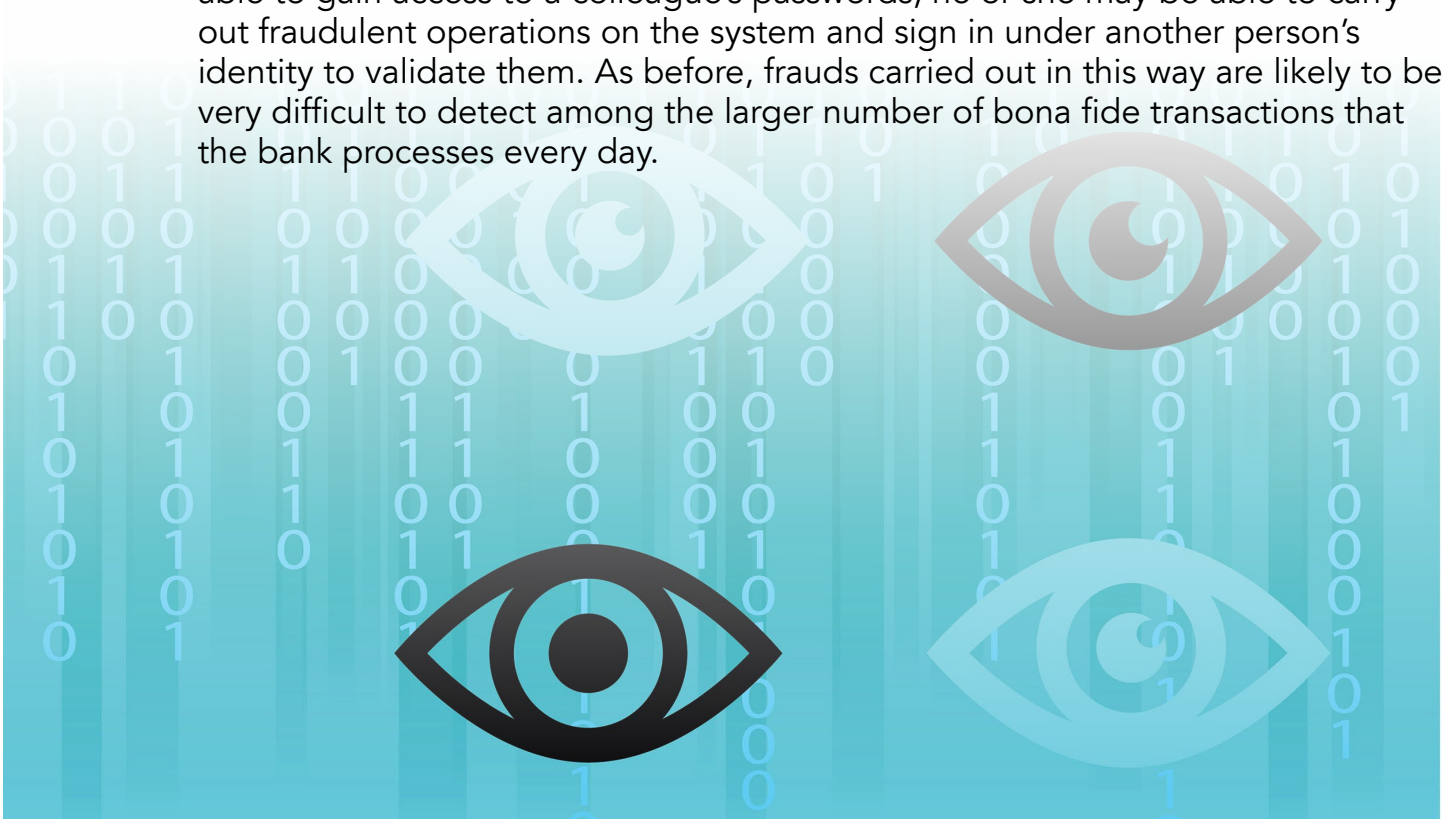
Amount looted by a criminal gang in the US in one extreme case of ATM fraud.

F Four eyes

The default method of validating a huge range of day-to-day procedures carried out within a bank is the so-called FOUR EYES principle. This simply means that operations carried out by one member of staff have to be validated by a second person to ensure they are in line with the bank's internal controls. In the majority of cases, this segregation of duties provides a simple way of ensuring that the bank's controls are effective and that rogue employees are not able easily to circumvent them.

However, the four eyes principle is clearly vulnerable to collusion between two or more employees who by acting together would be able to break down the normal segregation of duties and validate fraudulent transactions without raising any suspicions within the bank. Because frauds of this sort take place within the bank's existing system of controls they remain under the radar and are therefore extremely difficult to detect. Collusion between staff members therefore remains the easiest way to commit fraud within a bank.

Aside from direct collusion, employees may also be able to defeat the four eyes principle if there is poor password security within the bank. If a staff member is able to gain access to a colleague's passwords, he or she may be able to carry out fraudulent operations on the system and sign in under another person's identity to validate them. As before, frauds carried out in this way are likely to be very difficult to detect among the larger number of bona fide transactions that the bank processes every day.



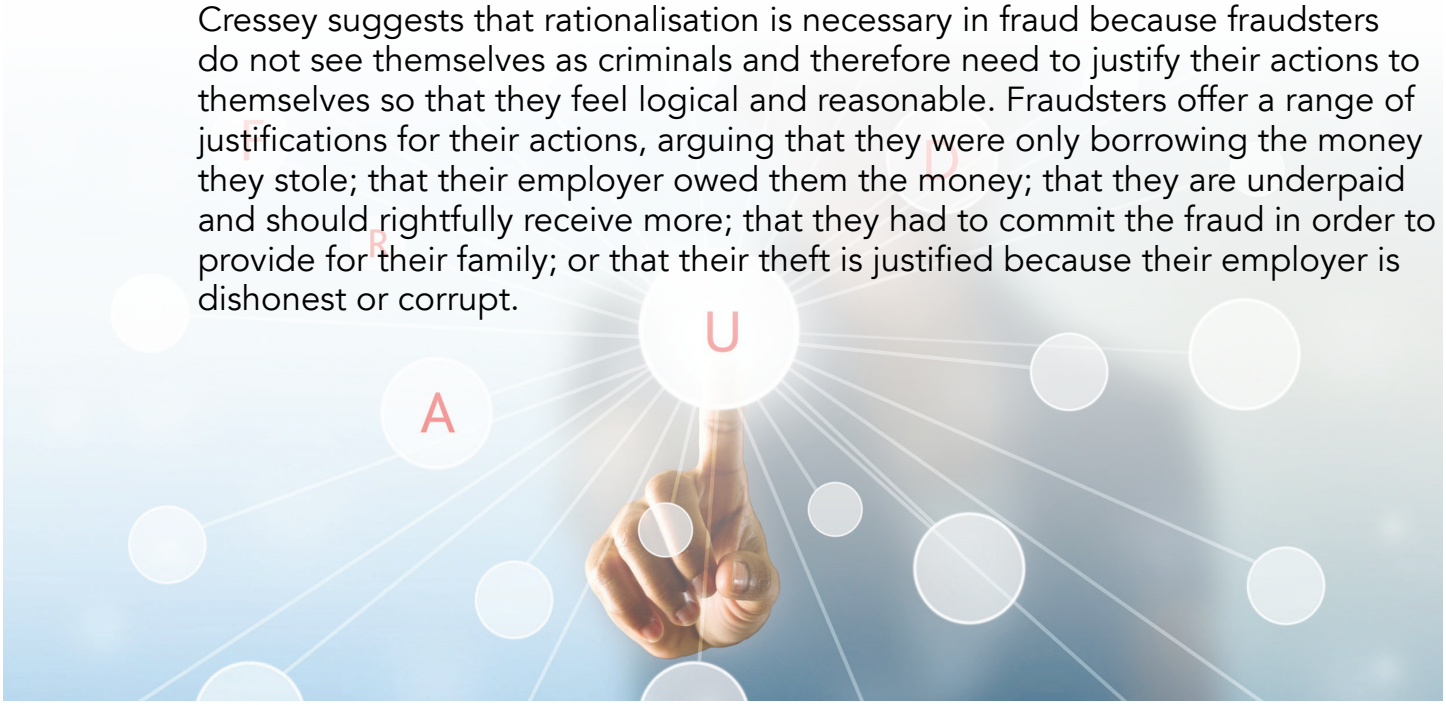
G Genesis of a fraud

The GENESIS OF A FRAUD committed in the workplace generally follows a pattern first identified by Donald Cressey, an American criminologist, in 1953. Cressey proposed the "fraud triangle", which sets out the three factors that need to be present for a workplace fraud to take place and is still in use some 60 years later.

Cressey's fraud triangle consists of pressure, opportunity and rationalisation. The first of these, pressure or incentive, describes the motivation that drives the employee to commit fraud, which can range from personal problems brought on by drink or drug abuse, relationship breakdown or gambling addiction, for example, to corporate pressures such as the need to demonstrate performance to superiors or outside stakeholders, such as investors or regulators. Alternatively, the incentive may be a breakdown in the employee's relationship with his or her managers, leading to a desire for revenge or a sense that legitimate worth and achievements are going unrecognised.

Opportunity can arise because of poor or non-existent internal controls or because the individual concerned occupies a position of trust that is vulnerable to abuse. If the fraudster can see an obvious way to cover their tracks they may well conclude that they have a good chance of making a substantial gain with a low risk of discovery.

Cressey suggests that rationalisation is necessary in fraud because fraudsters do not see themselves as criminals and therefore need to justify their actions to themselves so that they feel logical and reasonable. Fraudsters offer a range of justifications for their actions, arguing that they were only borrowing the money they stole; that their employer owed them the money; that they are underpaid and should rightfully receive more; that they had to commit the fraud in order to provide for their family; or that their theft is justified because their employer is dishonest or corrupt.



H Hacking

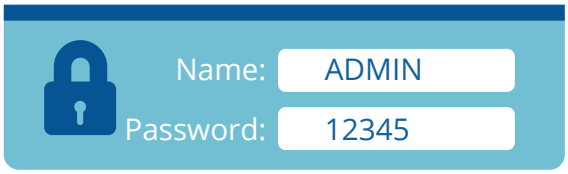
HACKING covers a huge variety of techniques used to find weakness in an organisation's IT security and so gain illicit access to computer systems for a range of reasons including fraud and data theft. At its simplest, hacking may involve nothing more than attempting to guess passwords, an approach that is more likely to succeed against organisations with poor controls on password security and those that do not demand users change their password regularly.

Hacking can also involve attempts to induce users to divulge their account information using email-based "phishing" attacks, or even fraudulent telephone calls that purport to come from the user's bank or financial services provider. Approaches such as these may simply involve gaining access to the victim's account in order to steal money but they can also provide the means to commit more intricate "identity theft", in which an individual's personal details are used to set up false accounts that are then used to obtain credit or make fraudulent purchases.

More sophisticated, technology-based types of hacking may involve attempts to introduce malicious software into the target organisation's computer systems, for example via email attachments, in order to capture sensitive information or to enable hackers to find a route into the system. The risks to cyber-security that hackers now pose have prompted the US ratings agency Standard & Poor's to warn in September 2015 that its credit ratings for banks will in future take into account the quality and strength of their IT security systems and procedures. "We view weak cyber security as an emerging threat that has the potential to pose a higher risk to financial firms in the future, and possibly result in downgrades," the agency said.

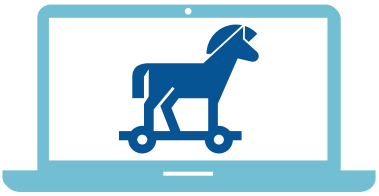
Hacking and how it's done

Covers techniques used to gain access to a bank's IT system with a view to carrying out fraud or data theft. Both sides are constantly at work: hackers devising new methods and software vendors finding ways to block the attacks.



Guesswork

More likely to succeed against organisations where there are poor controls on password security and where users are not required to change their passwords regularly

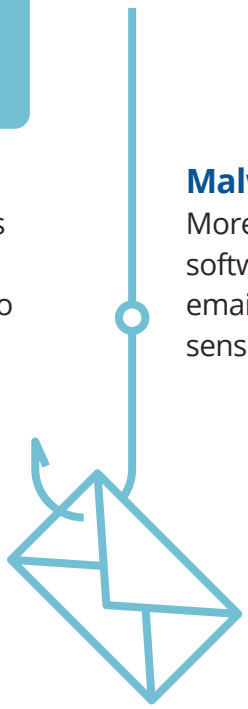


Malware

More sophisticated attacks introduce malicious software into a bank's computer systems, via email attachments for example, to capture sensitive information

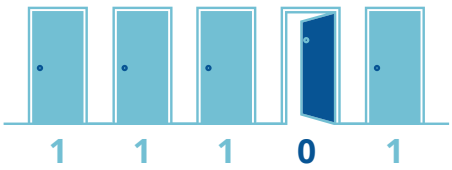
Identity theft

The victim's personal details are employed to set up false accounts that are then used to obtain credit or make fraudulent purchases



Phishing

Attempts to induce customers to divulge account information via email or even fraudulent phone calls that purport to come from the user's financial services provider



Zero day attacks

Take advantage of a previously unknown flaw in a widely-used piece of software, such as an operating system. These can go undiscovered for several years

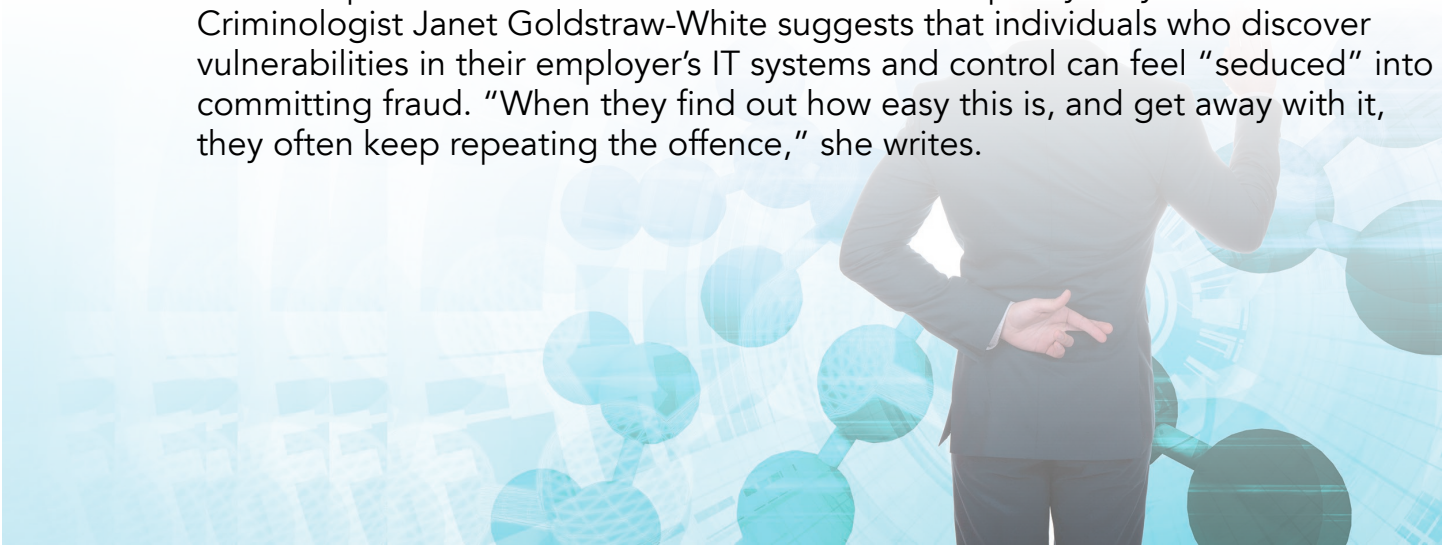
Standard & Poor's has warned that its credit ratings for banks will in future take into account the quality and strength of their IT security systems

I Internal fraud

INTERNAL FRAUD is the most common way for banks to suffer losses. Estimates vary, but PwC's Global Economic Crime survey for 2014 suggests that 56% of fraud is carried out by employees, though this encompasses a wider range of sectors than just banking. Others put the insiders' share of fraud cases within banking as high as 70%.

Employee fraud takes place at all levels of organisations. Survey data reported by the Economist Intelligence Unit show that among organisations that had suffered a fraud where the perpetrator was known, in 32% of cases the leading figure was a middle or senior manager while in 42% of cases it was a junior employee. In many cases involving banks, internal frauds will involve collusion between at least two individuals in order to circumvent the bank's controls, in particular the four eyes principle that is meant to ensure that one person carries out an operation while a second validates it. Employees with user privileges that give them high levels of access to the bank's IT systems, such as systems and database administrators, are particularly well placed to commit or facilitate fraud within banks and are often able to remove evidence of their actions from the system.

Fraud experts suggest that the process of carrying out a fraud usually takes place over a long period and will often start with an "exploration" of the bank's IT systems to see what the individual's access rights will allow them to do. They may look for a dormant account that will allow them to operate undetected or begin making small, temporary changes to the information on the system, such as a phone number, to see whether and how quickly they are detected. Criminologist Janet Goldstraw-White suggests that individuals who discover vulnerabilities in their employer's IT systems and control can feel "seduced" into committing fraud. "When they find out how easy this is, and get away with it, they often keep repeating the offence," she writes.



An inside job: who and why

Internal fraud is the most common way for banks to suffer loses and can take place at any level of an organisation. Roles with a high degree of access to IT systems, such as database administrators, pose a greater risk.

Cases in which the leading figure was a middle or senior manager

32%

42%

Cases in which the leading figure was a junior employee

Criminologist **Donald Cressey** identified a pattern in the way workplace fraud evolves. His "fraud triangle" consists of three elements: pressure, opportunity and rationalisation

Pressure

The employee's motivation to commit the crime, from personal problems such as drink, drugs or relationship breakdown to the need to out-perform colleagues or take revenge

Opportunity

Poor internal controls or the individual occupies a position of trust

Rationalisation

Fraudsters do not see themselves as criminals and so need to feel that their actions are logical and reasonable. They might argue they were "only borrowing" the money they stole or that their employer is corrupt

Many cases of internal fraud involve collusion between at least two individuals in order to circumvent the bank's controls

"When they find out how easy it is, and get away with it, they often keep repeating the offence"

Janet Goldstraw-White, Criminologist

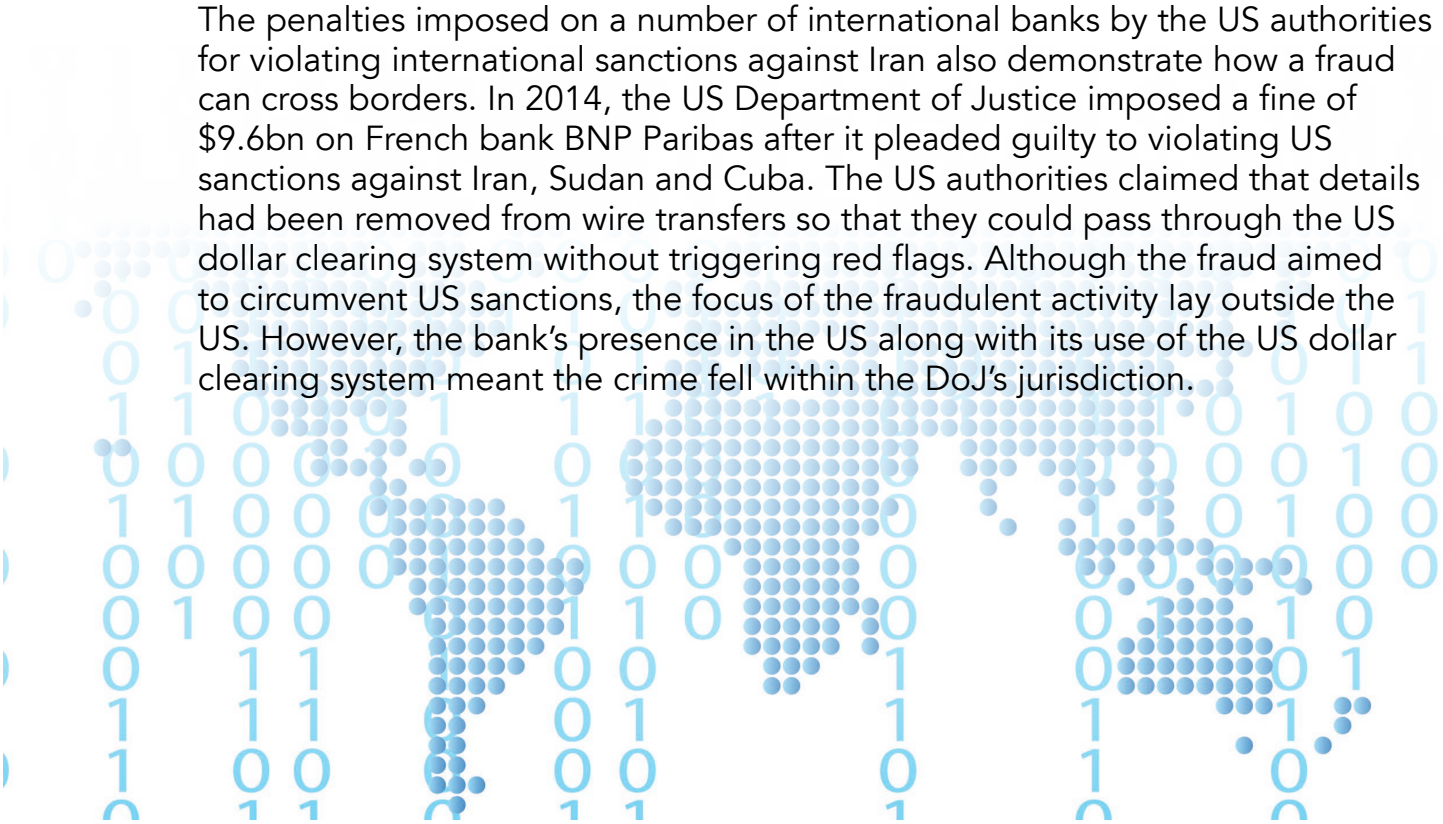
J Jurisdiction

The crime of fraud can often span more than one JURISDICTION, particularly where it involves multinational organisations such as large banks that have operations in numerous countries, or where elements of the fraud are directed from or carried out in another part of the world. Where frauds are carried out using digital information systems, it is possible that the activity may technically have taken place in more than one jurisdiction and so different countries' legal authorities could become involved.

In practice, legal authorities have demonstrated in recent cases that they are prepared to claim jurisdiction over activities that involved perpetrators operating from other territories, especially where these crimes involved global financial markets.

The fines imposed on US and European banks in May 2015 for their roles in attempting to rig foreign exchange markets are a case in point. The US Department of Justice and the UK's Financial Conduct Authority imposed fines totalling more than $5bn on a group of US and European banks, some of whose employees were involved in attempting to manipulate the FX markets.

The penalties imposed on a number of international banks by the US authorities for violating international sanctions against Iran also demonstrate how a fraud can cross borders. In 2014, the US Department of Justice imposed a fine of $9.6bn on French bank BNP Paribas after it pleaded guilty to violating US sanctions against Iran, Sudan and Cuba. The US authorities claimed that details had been removed from wire transfers so that they could pass through the US dollar clearing system without triggering red flags. Although the fraud aimed to circumvent US sanctions, the focus of the fraudulent activity lay outside the US. However, the bank's presence in the US along with its use of the US dollar clearing system meant the crime fell within the DoJ's jurisdiction.



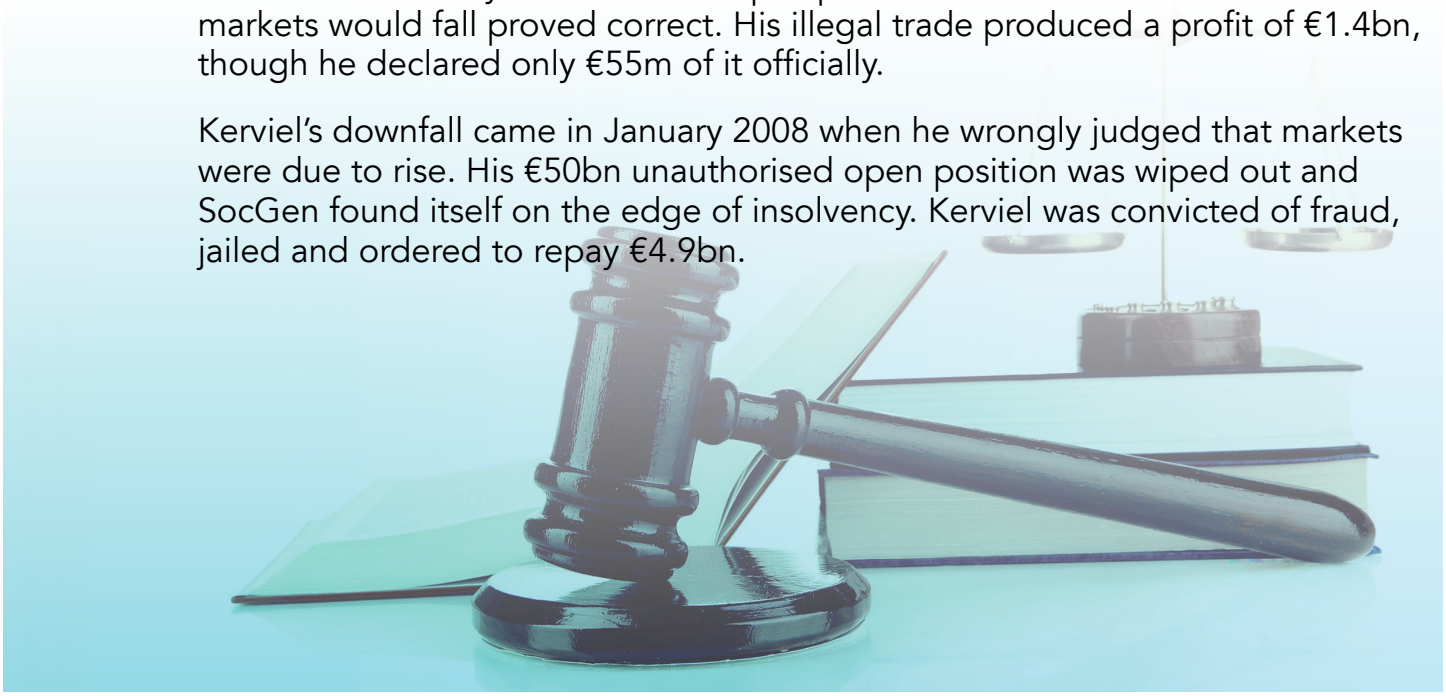
K Kerviel

Jérôme KERVIEL's name is forever associated with one of the most notorious cases of rogue trading within a large investment bank. The Frenchman worked at Société Générale in Paris between 2000 and 2008 and undertook a long-running fraud involving falsifying information about his trading positions, ultimately leading to the bank uncovering a loss of €4.9bn when Kerviel's bets that markets were due to rebound in 2008 proved disastrously wide of the mark. In the ensuing controversy, the bank's CEO resigned and it was forced into an emergency rights issue to repair its balance sheet.

Kerviel's first five years at SocGen were spent in the bank's middle office, where he entered trades carried out in the front office on to the bank's computer system. This enabled him to learn how the bank's controls worked and to discover ways to circumvent them. He was promoted to a trader after five years, and used knowledge gleaned in his previous role to build up huge unauthorised trading positions without being detected by the bank's compliance systems. Official accounts of his activities say that he covered his trades with matching fake hedges and closed them within a few days, just before the bank's automatic timed controls on traders' activities would have picked them up.

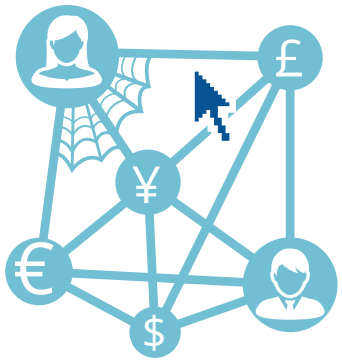
His unauthorised trading grew steadily more uncontrolled over time – in 2005 he made profits of €4m for the bank, in 2006 €11m, but in 2007 his activities increased massively – Kerviel built up exposure of €28bn and his bet that markets would fall proved correct. His illegal trade produced a profit of €1.4bn, though he declared only €55m of it officially.

Kerviel's downfall came in January 2008 when he wrongly judged that markets were due to rise. His €50bn unauthorised open position was wiped out and SocGen found itself on the edge of insolvency. Kerviel was convicted of fraud, jailed and ordered to repay €4.9bn.



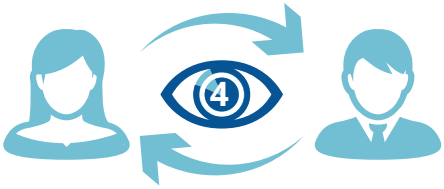
An inside job: how

Uncontrolled access enables fraudsters to steal or alter sensitive documents, execute illicit transactions and remove evidence of their activities. As the Cressey "fraud triangle" demonstrates, it can be a simple matter of opportunity...



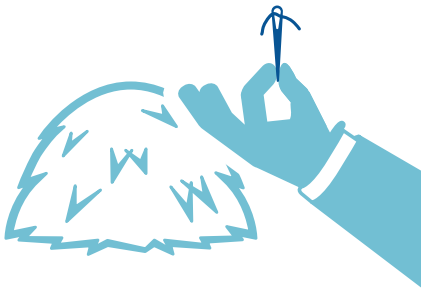
Experts suggest that the process of committing a fraud usually takes place over a long period and will often start with an "exploration" of the bank's IT systems by an individual to see what their access rights will permit them to do

They may look for a dormant account that will allow them to operate undetected or begin making small, temporary changes to information on the system to see whether and how quickly these are detected



Two members of staff operating in collusion can defeat the so-called "four eyes principle" – intended to ensure that one person carries out an operation while a second validates it

It's not rocket science, but a staff member who can access a colleague's passwords may be able to carry out fraudulent transactions on the system, then log in under that person's identity to validate them



Frauds carried out in this way are very difficult to detect amid the large number of bona fide transactions that the bank processes every day

A fraudster may seek to split a large transaction into multiple smaller ones that do not involve a breach of the bank's controls.

Respondents to a survey by the Economist Intelligence Unit who cited high staff turnover as an important source of vulnerability

L LIBOR

The illegal manipulation of LIBOR, the key market interest-rate benchmark, came to public attention in June 2012 when Barclays announced a settlement with US authorities worth $453m as recompense for its traders' involvement in the fraud. Libor – the London Interbank Offered Rate – is calculated daily on the basis of submissions by major banks and is meant to show the rate at which those banks are able to borrow from each other. This benchmark is used globally to calculate the price of up to $3.5 trillion of financial products, both wholesale and retail, ranging from complex derivative contracts to consumer mortgages and loans.

After the scandal broke it emerged that traders at a range of banks were colluding via private messaging systems to agree the interest rates that they would submit for the daily calculation of Libor, which at the time was carried out by the British Bankers' Association. Submitting slightly higher or lower figures could have a direct impact on the banks' profits via their trading activities, and therefore influence the profits and bonus entitlements of individual traders. For example, in a US class-action lawsuit filed in 2012, the plaintiffs alleged that banks colluded to ensure Libor increased on the first day of each month – the date on which new payment amounts on variable-rate mortgages were calculated, based on that day's Libor fix. Moreover, during the financial crisis, banks were able to mask the extent of their financial difficulties by colluding to depress Libor artificially, thereby giving the appearance that they could borrow more cheaply than was in fact the case.

Major banks have paid billions of dollars so far to settle cases related to Libor manipulation around the world, particularly in the US and UK, while some including UBS have received immunity for revealing details of the "Libor cartel" to prosecutors. In April 2015, Deutsche Bank paid US and UK authorities $2.5bn, the largest Libor settlement so far.

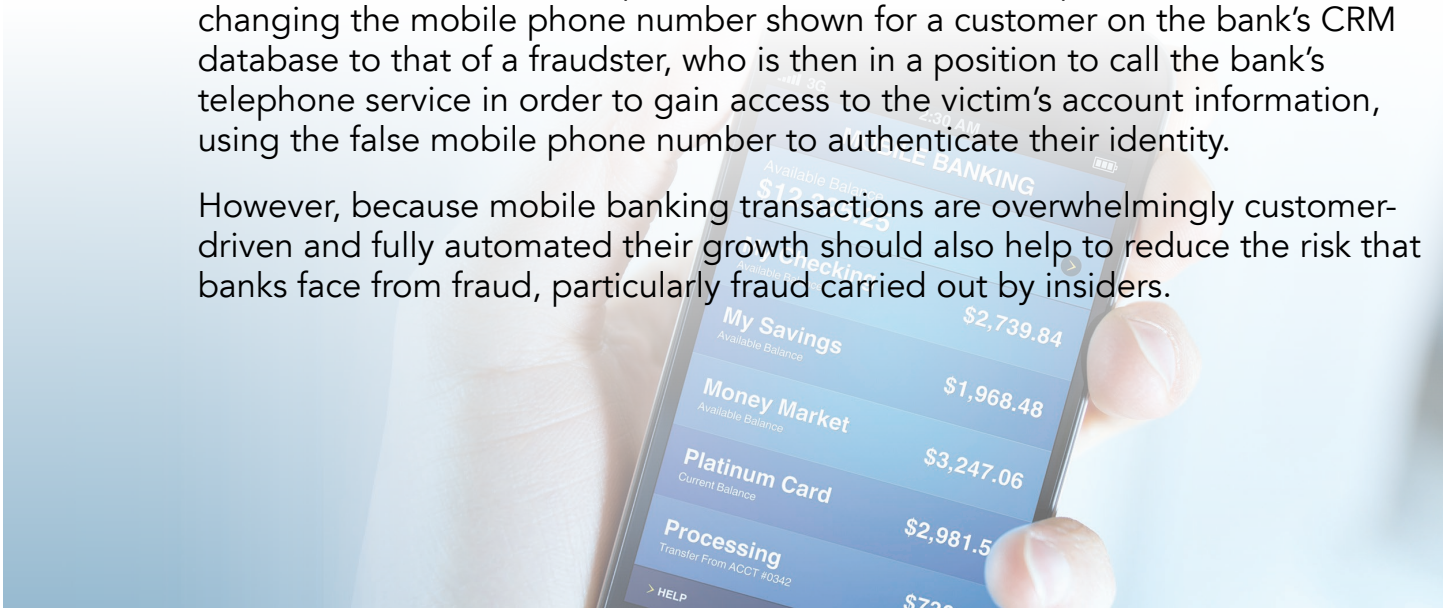
M Mobile

The rapid growth of MOBILE banking through phones and tablets reflects the central role that these devices now play in the lives of consumers around the world. It also highlights some of the growing challenges that banks face in handling their customers' migration to new banking channels. In the UK, research by the British Bankers' Association found that British consumers would use mobile devices to check their current accounts 895m times during 2015, against 427m transactions in bank branches. By 2020, the BBA forecast that customers will check their current accounts from mobile devices 2.3bn times a year, more than internet, branch and telephone banking combined.

As more consumers choose to make the mobile phone their primary method of managing most aspects of their day-to-day life, the potential clearly exists for banks to experience very rapid growth in customer numbers. The example of an African bank that saw its customer base grow from 4m to 14m in less than two years after it introduced mobile banking is far from unique. A shift of this size and speed inevitably places huge loads on the banks' IT systems as transaction volumes explode, as well as providing another route into the banks' information systems that can become vulnerable to fraud and unauthorised use. The hugely increased demands placed on staff and IT systems can make effective risk controls very difficult to implement and to scale up in step with rising customer numbers.

Mobiles are also becoming an important means to verify the identity of a customer, leaving the bank potentially vulnerable to simple frauds that involve changing the mobile phone number shown for a customer on the bank's CRM database to that of a fraudster, who is then in a position to call the bank's telephone service in order to gain access to the victim's account information, using the false mobile phone number to authenticate their identity.

However, because mobile banking transactions are overwhelmingly customer-driven and fully automated their growth should also help to reduce the risk that banks face from fraud, particularly fraud carried out by insiders.



N Near-Real Time

One of the greatest challenges to the effective use of big data analytics in detecting fraud is the time required to process the vast volumes of information involved. To be most effective, fraud systems need to be capable of NEAR-REAL TIME processing so that potentially fraudulent patterns of activity on the bank's IT systems can be detected rapidly and addressed.

Many banks currently run algorithms designed to detect fraud on the data in their core banking systems. The problem with this approach is that the data processing involved places a heavy load on the core banking system and will therefore tend to degrade its performance.

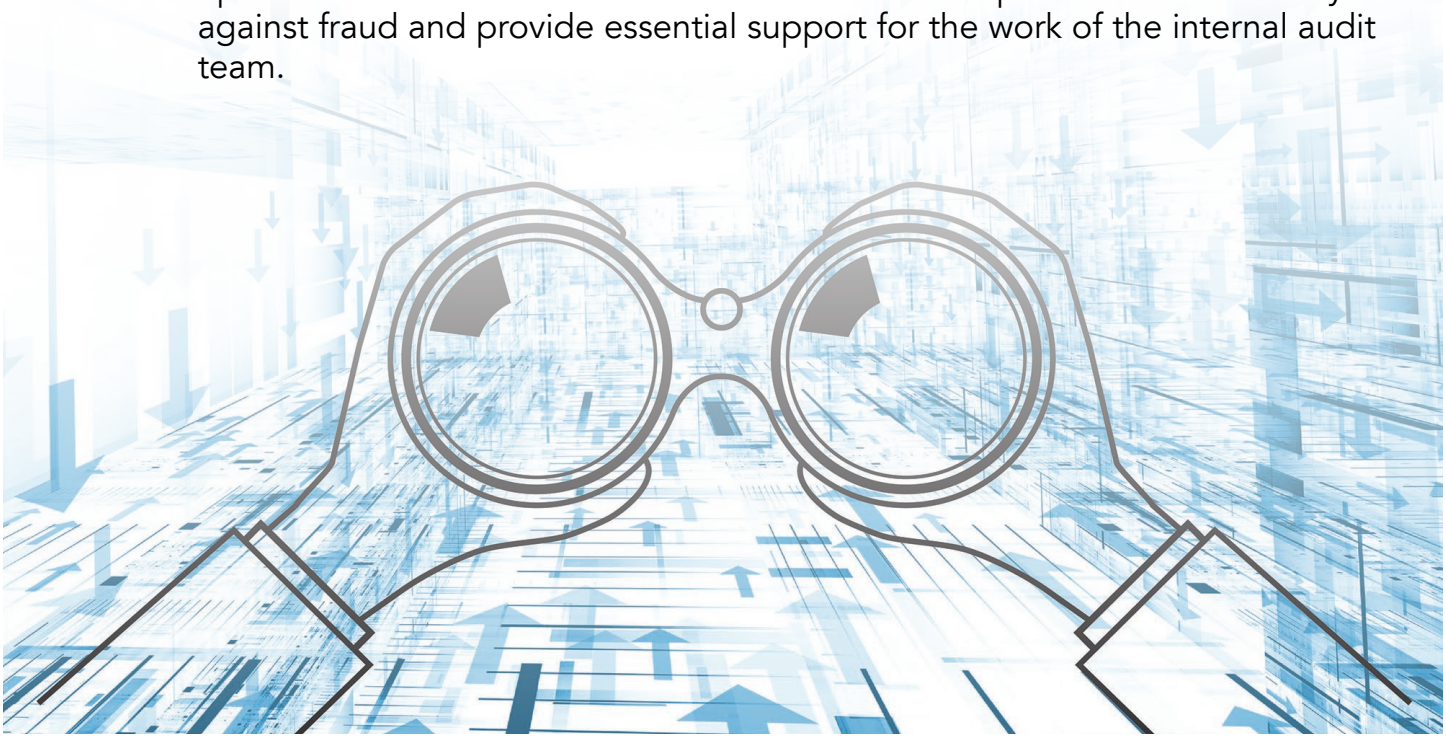
As a consequence, the algorithms cannot be run very frequently, leading to a lower level of anti-fraud protection. By contrast, using a more modern anti-fraud system that extracts the necessary data from the core banking system and analyses it in near-real time allows a much more proactive approach to fraud detection and prevention, as well as avoiding a negative impact on system performance.

O Oversight

OVERSIGHT of user activity lies at the heart of effective fraud detection and deterrence. It is based on the ability to detect activities that either breach internal controls, resulting in a "red flag" alert, or to identify patterns of activity that do not in themselves breach controls but that taken together indicate the possibility of fraudulent activity. In both cases, effective monitoring of the use of the bank's technology systems by thousands of individuals and interpreting their behaviour is the key to effective fraud detection and reporting.

Where employees in particularly sensitive jobs are concerned, specialist systems can be put in place to provide an added level of assurance in areas where banks have potentially serious vulnerabilities. In particular, specially designed systems are available to monitor the activities of systems administrators and database administrators on the bank's IT platform and reduce the risk of frauds carried out by system users with very high access privileges.

The critical role that technology now plays in anti-fraud oversight has also brought about big changes in the way that banks' internal auditors need to operate and the skills they require to do their jobs. Auditors are frequently drawn from the operational side of the bank and may therefore lack detailed knowledge of how the bank's IT systems work and their potential vulnerabilities. Specialist IT auditors have therefore become a vital part of banks' armoury against fraud and provide essential support for the work of the internal audit team.



P Profiling

In cases where fraudulent activity does not involve a violation of any of the bank's internal controls – and therefore does not trigger a red flag alert on its security systems – PROFILING offers one of the most effective counter-measures. This aspect of big data analytics is akin to machine learning, in that the anti-fraud system will analyse large bodies of data over time in order to establish patterns relating to particular accounts and customers that reflect their normal behaviour.

In a simple example, this might involve payments into an account on a particular day of the month from a regular source such as an employer, withdrawals from ATM machines within a typical geographical area and purchases of a typical average size from a range of offline and online sources. By assembling data of this sort over a period, the system can create a notional profile of that customer or account against which to evaluate and query transactions that appear to fall outside of the recognised parameters.

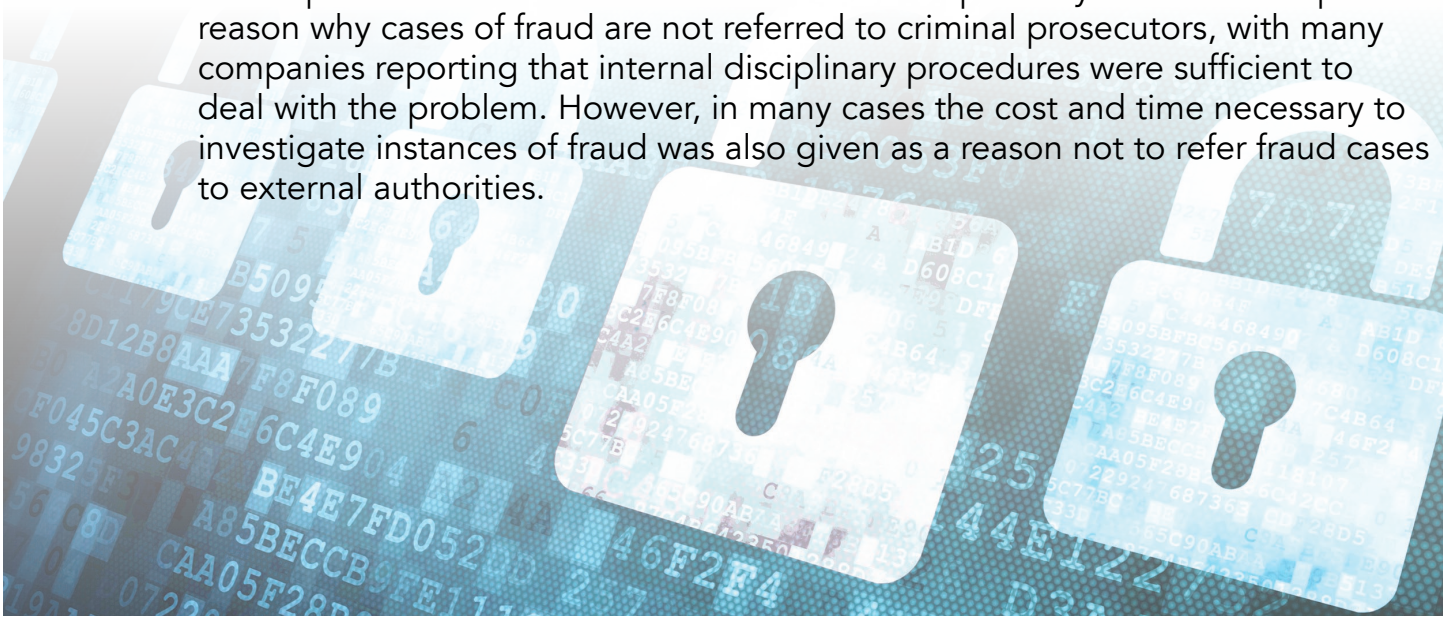
These might involve an ATM withdrawal or card payment in a different country, a transaction of an unusual size or one that takes place at an unexpected time of day. In an investment banking context, profiling of the net positions and trading activity of a group of traders might enable a bank to identify whether any of them shows a pattern of activity that differs from colleagues working in the same team. Ultimately, the ability to create profiles in this way will enable anti-fraud systems to carry out ongoing predictive analysis of user behaviour and transaction patterns as they occur in order to give early warning of suspect activities.

Q Quantum

The QUANTUM of fraud committed against banks is hard to determine precisely, since many cases go unreported. However, in its Report to the Nations, 2014, the Association of Chartered Fraud Examiners estimated that banking fraud in that year amounted to $67bn, approximately 6% of the total pre-tax profits of the top 1,000 institutions. Some 70% of this is said to have resulted from frauds carried out by insiders. The association works across a wide range of industries but its findings indicate that banking and financial services have by far the highest incidence of fraud of any sector it examines, accounting for 17.8% of cases compared with 10.3% for the next highest category, government and public administration. Further evidence comes from the 2014 US State of Cybercrime Survey, which found that the number of financial firms reporting losses of between $10m and $19.9m jumped by 141% year on year.

According to survey work by the Economist Intelligence Unit, in 2012-13 three-quarters of financial services companies globally experienced at least one fraud and on average these businesses incurred losses equivalent to 1.5% of their revenues. Data theft and internal financial fraud both affected about 30% of financial services companies, regulatory and compliance breaches occurred in 26% and money laundering in 8%. Respondents who took part in the EIU study cited IT complexity as the top risk factor that their organisation faced, although almost 40% said that high staff turnover was another important source of vulnerability.

The Report to the Nations found that fear of bad publicity is the most important reason why cases of fraud are not referred to criminal prosecutors, with many companies reporting that internal disciplinary procedures were sufficient to deal with the problem. However, in many cases the cost and time necessary to investigate instances of fraud was also given as a reason not to refer fraud cases to external authorities.



R Regulators

REGULATORS are putting all financial services companies under increasing pressure to ensure that they are doing enough to protect sensitive customer data from accidental loss or theft, and to demonstrate that they are doing so. In the past, much regulation on data security has been "declarative", requiring firms simply to confirm that they comply with the rules. Now newer regulations are forcing organisations to prove that this is the case. This is an important shift and significantly increases the compliance burden that companies face.

New rules on cyber security and data protection are emerging from both national regulators and at the European level, among them the EU General Data Protection Regulation, which is expected to come into force in 2018, and rules on protecting client identifying data from the Swiss regulator, FINMA, that follow serious data breaches at banks including HSBC in Geneva. The GDPR rules will place new obligations on organisations, and professionals polled by the UK publication Computer Weekly in summer 2015 believed that banks operating in the European Union would be the first group to come under scrutiny by regulators seeking to tighten up standards of data security.

The regulations will require any data security breach to be reported to regulators within 72 hours and in the most serious cases will enable regulators to impose fines of up to 2% of global turnover. Banks will also be responsible for their confidential data when it is in the hands of third-party suppliers and outsourced service providers, requiring them to carry out enhanced due diligence and compliance checks.

S Straight through processing

As IT systems have progressively automated the majority of repetitive, everyday transactions that banks carry out, the use of STRAIGHT THROUGH PROCESSING, where there is no human involvement in the transaction, has allowed new fraud risks to emerge. Straight through processing obviously brings great cost and efficiency advantages for banks by enabling them to handle higher volumes of transactions, but it also puts huge emphasis on the strength and effectiveness of the internal control systems that they use to monitor these billions of automated transactions.

If these controls are weak or contain flaws, it will be possible for fraudulent transactions that do not involve a direct breach of any internal control to be completed without triggering a security alert. These frauds may never be detected, and even when they are it may be too late to take any effective action. A fraudster may seek to split a large fraudulent transaction into multiple smaller ones to ensure that none of them individually raises questions. Unless the bank has systems that will sound an alert if an unusually large number of transactions are taking place on the same customer account or linked accounts, it is likely that a fraud attempt like this could succeed without raising a "red flag" alert. Where transactions take place that do not involve a breach of the bank's controls, monitoring systems that analyse the behaviour of system users in order to detect patterns known to be connected with fraudulent activity provide the critical line of defence.

T Transaction Analytics

In modern banking, where huge numbers of standardised transactions are automated through straight through processing, the need to implement and enforce a well-structured set of controls is paramount. These automated controls constitute the first line of the bank's technology-based defences against attempts to carry out fraudulent transactions because they define the parameters of legitimate activity.

However, in order to ensure that the automated controls built into the bank's IT systems are operating effectively and are not being over-ridden or bypassed, they must be constantly monitored. TRANSACTION ANALYTICS is the process of carrying out this monitoring so that any breaches of the bank's system of controls will result in security alerts being raised to enable appropriate action to be taken. In effect, therefore, using transaction analytics enables a bank to automate part of its internal audit process and ensure that it is applied continuously.

Transaction analytics offers a major advantage over traditional methods of checking internal controls in that it can be applied to every transaction that the system processes. Previously, manual sampling was used to check that controls were being applied properly, with the results of the sample being used to draw conclusions about the system overall. However, not only is manual sampling labour-intensive, slow and expensive, it also leaves the majority of transactions untouched. By automating the process of analysing transactions to detect breaches of controls, banks can achieve a much greater level of scrutiny than traditional methods allow.

U

U.B.A.

USER BEHAVIOUR ANALYTICS (UBA) is a fast-emerging area of fraud detection within banks. It is based upon big data analysis and requires the ability to assess very large volumes of data from multiple sources within the bank's IT systems. This is analysed at the level of individual users and banks also seek to identify links between users and entities on the system. Once the UBA system has been configured to reflect the working practices of an institution and has established a baseline for its users' typical behaviour, it is able to identify anomalous examples, whether carried out by insiders or external intruders, and flag them for further investigation.

This area of fraud detection is still developing and to date has varied significantly from one provider to another. The important trends in this market include the level and extent of data analysis that the bank is required to carry out internally. More advanced UBA systems now include large suites of so-called "canned analytics", meaning that the system provides information to the bank in a readily useable form, for example via dashboards. Banks therefore do not require their own data scientists in order to make proper use of it. UBA providers are also increasingly providing these systems as a service, whereby the provider's staff carry out analysis and forward reports of anomalous activity to the customer.

V Volume

One of the biggest challenges that any bank faces today in attempting to detect and counteract fraud is the vastly increased VOLUME of digital traffic that its systems have to handle each day. As banking becomes increasingly digital rather than cash-based and the market penetration of financial products from mortgages to credit cards increases, the volume of transactions that must be processed electronically through the bank's IT systems each day – which can already number 20m or more for a large organisation – will continue to climb.

Until relatively recently, many banking operations were still processed manually on paper, which made the checking and verification process slower but less vulnerable to abuse. However, the increase in digital transaction volumes has made this approach untenable. Instead, banks have been forced to automate as many routine processes as possible to accommodate high volumes of digital transactions.

This inevitably means that most transactions will no longer undergo any human checking, enabling fraudulent activity to slip through the bank's systems provided it does not contravene any internal controls. This also increase the risk of "false positives" – legitimate transactions that trigger a fraud alert and require staff time in order to confirm they are not a threat. A well-structured and well-monitored system of controls is therefore vital in enabling huge volumes of transactions to be processed safely. But as the speed and quality of Big Data Analysis rapidly improves, sophisticated fraud detection systems are also becoming central to the effort to detect and prevent frauds hidden among the millions of operations that take place every day.

Alongside the continuing increase in digital transaction volumes, the growing adoption of mobile banking is pushing up the number of customer queries that bank systems must deal with because mobile customers tend to check their balance and recent transactions much more frequently than people banking via other channels. Recent estimates by the British Bankers' Association suggested that UK customers would access their accounts via mobile banking 895m times in 2015, rising to 2.3bn in 2020. This will not necessarily result in a higher overall volume of transactions, but it will undoubtedly place additional burdens on the bank's IT infrastructure.

W Whistleblowing

WHISTLEBLOWING is the main initial source of information leading to the detection of frauds carried out by employees of public and private sector organisations, accounting for more than 40% of cases according to the 2014 Global Fraud Study, published by the Association of Certified Fraud Examiners. These findings cover all industries but remain directly relevant to banking.

In view of the central importance of tip-offs in detecting fraud, banks must put in place procedures to ensure that they are able to derive the maximum possible benefit from information passed to them by informants. The first step is to see that the organisation has a well-structured policy on whistleblowing that enables staff who come forward to feel confident that they will not be victimised or see their career prospects compromised if they reveal wrongdoing. Whistleblowers have frequently suffered as a result of their actions because their superiors do not want incidents of wrongdoing or fraud to be revealed and risk damaging the organisation's reputation and brand. Any whistleblowing policy must therefore offer credible reassurance to staff, and its existence must be widely communicated so that people are aware of the protection it can offer. Equally, however, the organisation must take steps to protect itself against malicious accusations and experts usually recommend that fraud tip-offs from insiders should be treated as confidential, rather than accepted anonymously.

Equally, it is important for banks to realise that many tip-offs originate from outside the organisation: from customers and suppliers, for example. Many banks therefore maintain a dedicated fraud desk to receive customers' tip-offs and block accounts that have been compromised. In June 2015, the Nigerian Central Bank ordered all the country's banks and payment providers to set up fraud desks as a key part of their defences. Combined with a well-structured system of internal controls and advanced anti-fraud software, whistleblowing has a vital role to play.

X XXL

Technology enables banks to operate with very high transaction volumes, but the same is also true of fraudsters. This means that a single fraud can have an XXL impact, resulting in huge losses. In one extreme case of ATM fraud uncovered in the US, a criminal gang looted $45m from cash machines around the world in two separate attacks. The gang first hacked into databases containing details of prepaid debit cards belonging to two banks based in the Middle East. The hackers collected debit card data, removed withdrawal limits on the accounts and created access codes. They were then able to use the account data and fraudulent access codes to enable any plastic card with a magnetic strip to withdraw cash from the compromised accounts.

In their second, much larger attack the gang passed information to groups of fraudsters in cities around the world who then moved from one ATM to the next, withdrawing huge sums. In the space of just a few hours, more than 36,000 fraudulent withdrawals were made resulting in the theft of about $40m.

Information on the theft became public when eight members of the New York-based cell involved in the fraud were brought to trial. The case highlighted a range of vulnerabilities that the fraudsters were able to exploit, including the lack of security and screening technology at the banks involved that could have helped them to detect and counteract the hackers. Also, the continued use in the US of cards with magnetic strips enabled fraudsters to produce working versions using false access codes very easily. These magnetic cards have been abandoned in most other countries and are now being phased out in the US as well in favour of chip-and-pin technology, which is more difficult to copy, but because US banks and merchants still used magnetic cards they continued to be accepted in other parts of the world.

Y Youth

In the past two decades the rapid spread of the digital economy has exponentially increased the quantities of data that organisations generate and with it the challenges of maximising the value of these vast pools of information. In January 2009, Hal Varian, Google's chief economist, told McKinsey Quarterly: "I keep saying the sexy job in the next 10 years will be statisticians…The ability to take data – to be able to understand it, to process it, to extract value from it, to visualise it, to communicate it – that's going to be a hugely important skill in the next decades." Anti-fraud technologies that depend on these crucial skills are still in their YOUTH – many were developed only in the past few years and in many cases banks have only recently begun pilot projects that use modern techniques such as big data analytics. There is much further to go before these technologies become a routine part of how banks operate day-to-day: in early 2014, the technology market analyst Gartner said that just 8% of large, global companies had adopted big data analytics for at least one security or fraud detection use case. It forecast that the proportion would increase to one-in-four.

These new technologies are developing quickly, which brings both opportunities and challenges for organisations that want to take advantage of them. On one hand, the rapid evolution of systems will require banks to adapt and update their controls frequently and undertake continuous training to stay abreast of technological developments and the evolution of techniques for committing fraud. On the other, as anti-fraud systems evolve they are continuing to improve. Increased processing power is enabling them to become faster and more intelligent, and the quality and user-friendliness of the analysis they provide to security staff are improving, making them easier to use. Banking is becoming ever more dominated by digital technologies and as this process continues, technology will inevitably be an indispensable weapon in the constant fight against fraud.

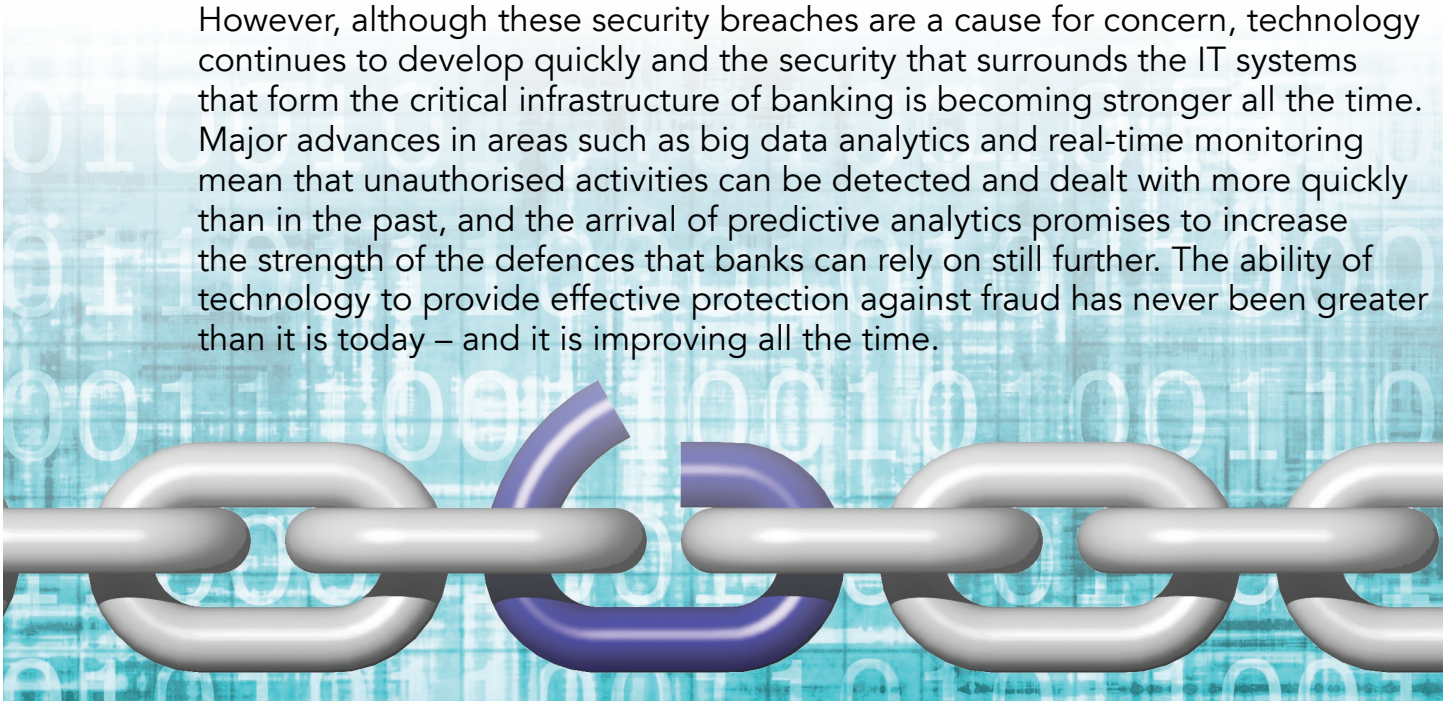
Z Zero day

The battle between institutions and fraudsters resembles an arms race. Technology developers are at work on both sides: hackers creating new ways to penetrate IT systems to steal information and carry out fraudulent transactions, while software vendors work to block these attacks and discover new vulnerabilities in their programs before the hackers do.

Occasionally, hackers succeed in exploiting holes in the software systems that organisations use before IT security staff become aware of the weakness. These are known as ZERO DAY attacks and refer to the taking advantage of a previously unknown software flaw. There have been zero day attacks on widely used pieces of software including PC and Mac operating systems and web browsers. Software vendors release thousands of security patches to plug the holes that are discovered in their code, but in some cases they are discovered only when people suffer an attack.

It can take years for a zero day attack to be discovered. The Red October malware went undiscovered for five years, during which time it was used to steal information from governments, embassies, energy companies and nuclear installations in 39 countries. It was uncovered in October 2012 by the Russian security company Kapersky Labs. The creators planted the malware in Microsoft Word and Excel documents that were sent to target recipients by email.

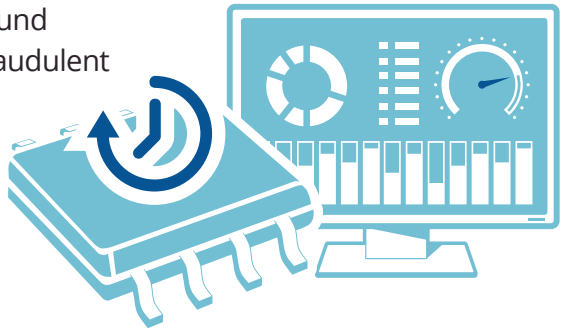
However, although these security breaches are a cause for concern, technology continues to develop quickly and the security that surrounds the IT systems that form the critical infrastructure of banking is becoming stronger all the time. Major advances in areas such as big data analytics and real-time monitoring mean that unauthorised activities can be detected and dealt with more quickly than in the past, and the arrival of predictive analytics promises to increase the strength of the defences that banks can rely on still further. The ability of technology to provide effective protection against fraud has never been greater than it is today – and it is improving all the time.



The soon to be future

Oversight of user activity lies at the heart of fraud detection and deterrence. Trust will remain key, but technology to track criminal behaviour is ever improving – just as new rules are unveiled to further regulate the industry.

Real-time processing is around the corner and will allow fraudulent activity to be detected and addressed as it happens



User behaviour analytics are developing fast and will deliver information in a readily-usable form without the need to employ specialist data scientists – via a "dashboard" display, for example

For employees in sensitive jobs – such as systems and database administrators – tailored systems can now be put in place to reduce the risk among users with very high access privileges

The critical role that technology plays in anti-fraud oversight means changes to the way internal auditors operate and the skills they require. Specialist IT auditors are becoming a vital part of every bank's armoury

Volume of fraud cases that first come to light as a result of whistleblowing. To derive maximum benefit from tip-offs, banks have to change their attitude and establish new procedures

(Source: 2014 Global Fraud Survey)

2018
Year when the EU General Data Protection Regulation is expected to come into force

72 hours
Maximum time allowed for breaches of data security to be reported under the new GDPR rules

2%
of global turnover proposed as the maximum fine

About Temenos

Temenos Group AG (SIX: TEMN), headquartered in Geneva, is a market leading software provider, partnering with banks and other financial institutions to transform their businesses and stay ahead of a changing marketplace. Over 2,000 firms across the globe, including 38 of the top 50 banks, rely on Temenos to process the daily transactions of more than 500 million banking customers as well as over USD 5 trillion in assets.

Temenos customers are proven to be more profitable than their peers: in the period 2008-2012, they enjoyed on average a 32% higher return on assets, a 42% higher return on equity and an 8.1 percentage point lower cost/income ratio than banks running legacy applications.

About NetGuardians

NetGuardians is a leading banking software company recognized for its unique approach to fraud and risk assurance solutions. Our award-winning software leverages Big Data to correlate and analyze behaviors across the entire bank system – not just at the transaction level. This broader vision is the secret to our creative edge. We earn the confidence of our clients by combining the technical know-how of our R&D team with our in-depth understanding of the evolving risk challenges faced by banks in a border-free world.

Founded in 2007, NetGuardians was the first company to emerge from the innovation incubator Y-Parc, in Yverdon-les-Bains, Switzerland. The company now enjoys a solid international presence with a steadily growing clientele in Europe, Middle East and Africa. In 2015, NetGuardians has been named a Gartner "Cool Vendor" in "Cool Vendors in Audit and Compliance Innovate Controls Validation Techniques":

http://www.netguardians.ch/gartner