NetGuardians

A-Z

# of Internal Banking Fraud

Contents

Introduction

It is no exaggeration to say that the greatest fraud risk that banks face walks through their doors every morning and sits down to work

Frauds carried out by bank employees are a huge global problem. Recent research puts the cost of banking fraud at around $70bn a year – and cases involving bank insiders account for about 70 percent of that total. The A-Z of Internal Banking Fraud highlights the scale of this problem and the different vulnerabilities that internal fraudsters exploit, and explains how advanced anti-fraud technologies can combat it. Bank employees are uniquely well placed to discover and take advantage of weaknesses in their organization's internal controls – perhaps by abusing their level of access to the bank's IT systems or by targeting dormant accounts.
But FinTech anti-fraud solutions are improving all the time – their ability to identify and block suspicious activity in real time is becoming the first line of defense against the biggest fraud risk in banking.

> “
>
> **Recent research puts the cost of banking fraud at around $70bn a year**

A

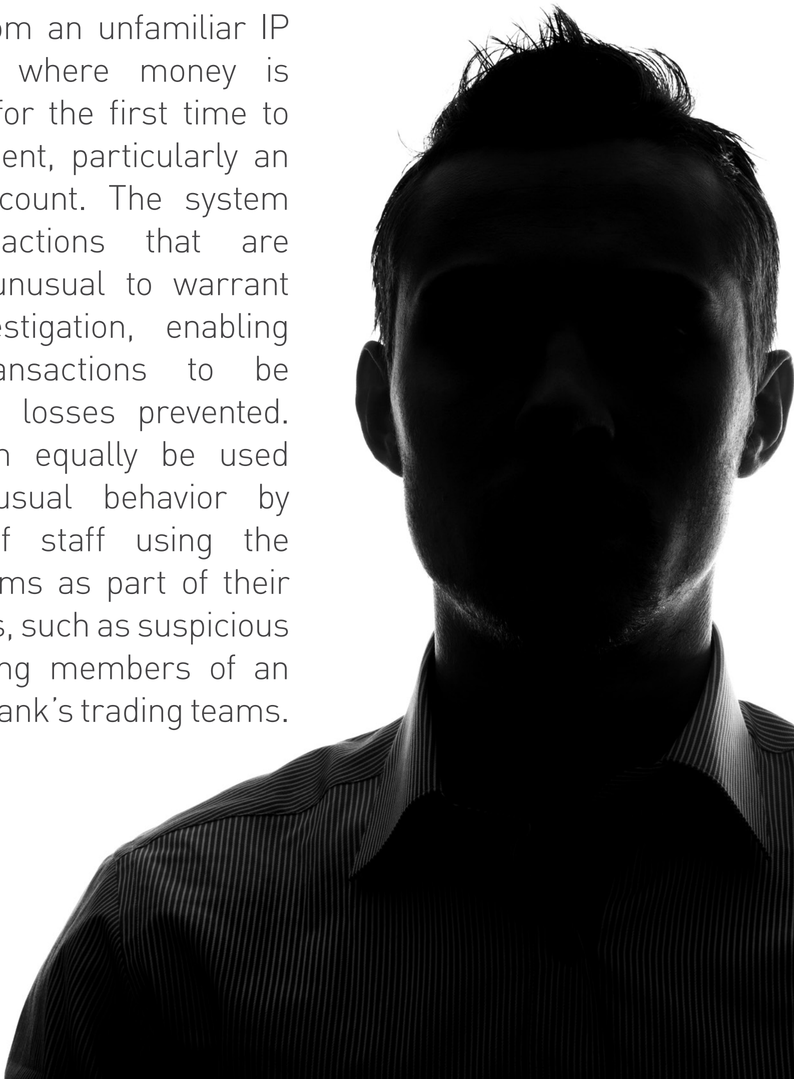
Abuse of Administrator Privileges

Abuse of administrator privileges is one of the key internal-fraud risks facing financial institutions. It represents an unavoidable source of difficulty because some highly trusted IT staff will always require "super-user profiles" to perform their everyday duties or carry out essential maintenance on the core banking systems. Even though system administrators do not normally need to go into the live "production environment", their high-level access inevitably creates opportunities to carry out or validate fraudulent transactions. Problems can arise when IT departments neglect to remove temporary "extended rights" from staff after a specific project finishes, leaving them with greater access to the core system than they should rightly enjoy. Given that banks tend to check user access profiles only monthly or quarterly, an oversight like this can allow a rogue employee enough time to commit a fraud. Abuse also occurs through collusion between IT staff and others, such as front-office employees: a system administrator might grant a super-user profile to a front-office colleague for just long enough to create and approve a fraudulent payment, then remove the access privileges again. Historically it has been difficult to monitor the activities of individual IT administrators because they use generic logins, but modern anti-fraud technology overcomes this problem by requiring each administrator also to sign in to a proxy account using their own credentials. Thus a complete audit trail can be maintained for every one, enabling suspicious changes to user profiles to be flagged.

Behavioral Profiling

B

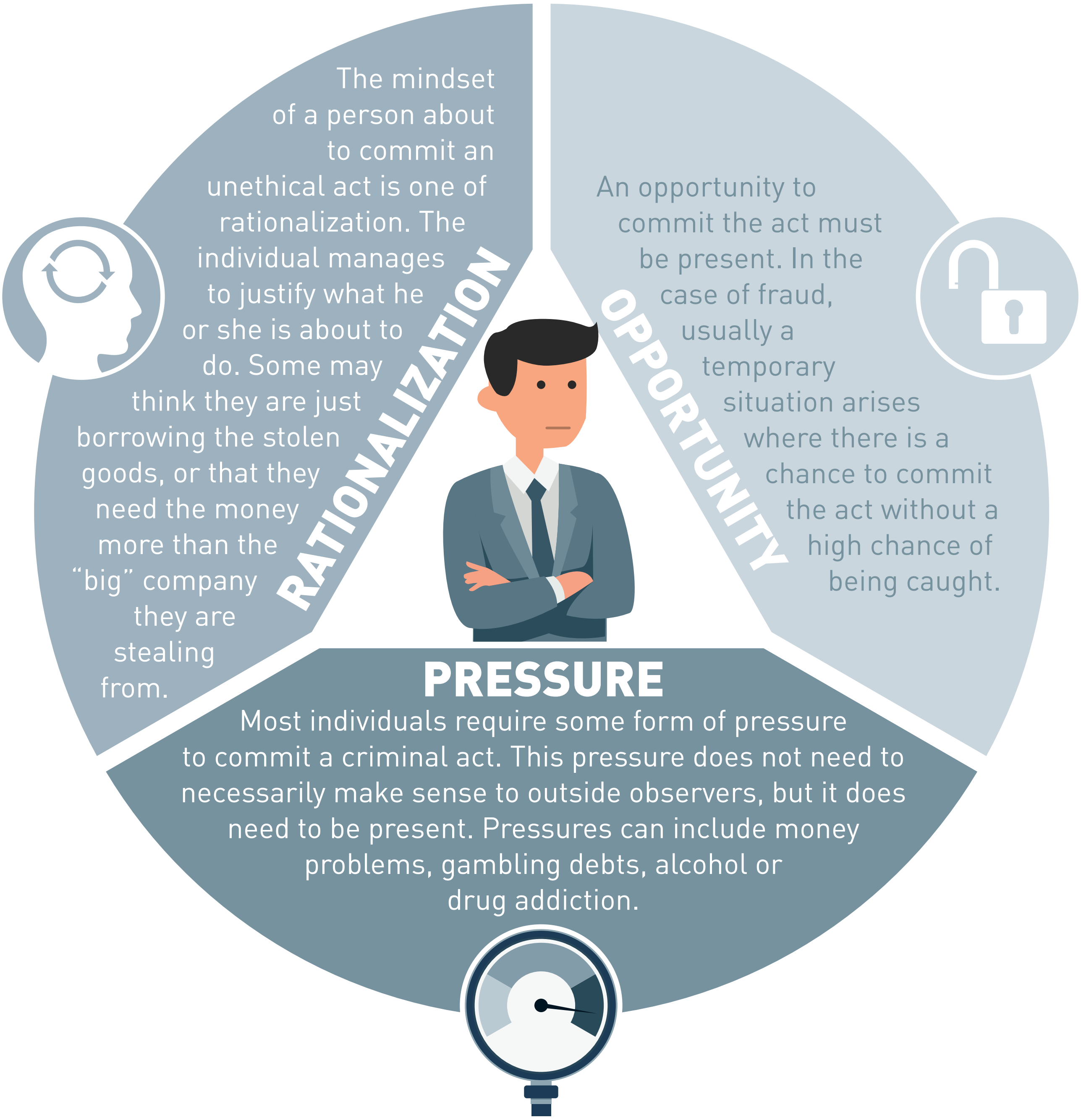
Behavioral profiling lies at the heart of technology-based anti-fraud systems and represents a major recent advance in fraud detection made possible by the increasing power of Big Data analytics. Profiling complements rule-based controls by analyzing very large amounts of data on the historical behavior of each employee and customer to create a profile that describes the typical way in which they use their account: how, when and where they access it; who they usually make payments to; the sums normally involved; and so on. The system then compares each action that takes place on the account against the profile and scores it against a range of risk indicators to estimate the probability that the transaction is a result of internal or external fraud. For example, profiling will highlight cases where an account is accessed from an unfamiliar IP address or where money is transferred for the first time to a new recipient, particularly an overseas account. The system flags transactions that are sufficiently unusual to warrant further investigation, enabling suspect transactions to be blocked and losses prevented. Profiling can equally be used to flag unusual behavior by members of staff using the bank's systems as part of their everyday jobs, such as suspicious activity among members of an investment bank's trading teams.



C

Cressey's Triangle

Conceived by American criminologist Donald Cressey as a model to explain workplace fraud. It comprises the three elements Cressey argued must be present for internal fraud to occur: **Pressure**, **Opportunity** and **Rationalization**.



RATIONALIZATION

The mindset of a person about to commit an unethical act is one of rationalization. The individual manages to justify what he or she is about to do. Some may think they are just borrowing the stolen goods, or that they need the money more than the "big" company they are stealing from.

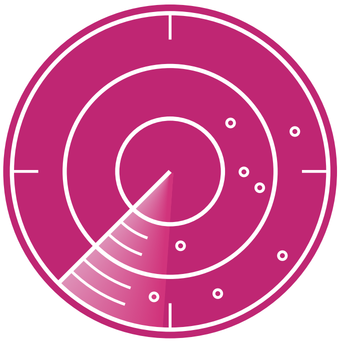
OPPORTUNITY

An opportunity to commit the act must be present. In the case of fraud, usually a temporary situation arises where there is a chance to commit the act without a high chance of being caught.

PRESSURE

Most individuals require some form of pressure to commit a criminal act. This pressure does not need to necessarily make sense to outside observers, but it does need to be present. Pressures can include money problems, gambling debts, alcohol or drug addiction.

D



Detection

“

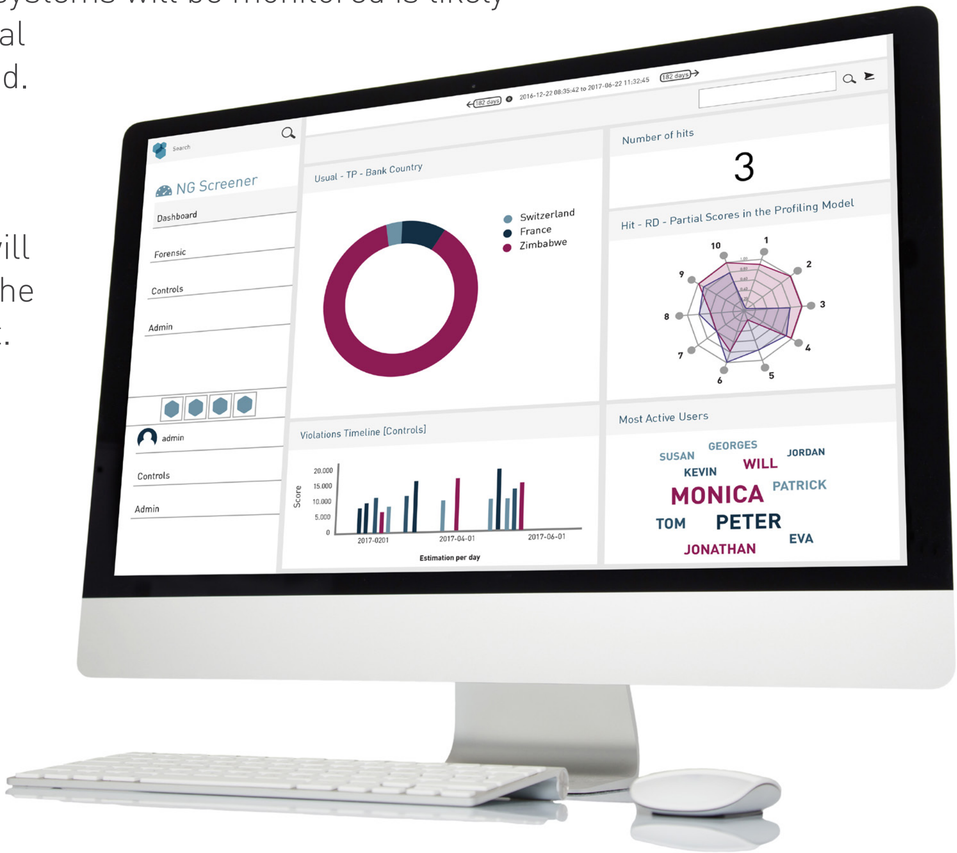
The most common method of detection is informal tip-offs from other staff or customers

Research by a number of different organizations reveals that internal fraud is detected in a wide variety of ways. Both the Association of Certified Fraud Examiners (ACFE) and KPMG, in its report *Global Profiles of the Fraudster 2016*, find that the most common method of detection is informal tip-offs from other staff or customers, although a large proportion of internal frauds come to light via whistle-blowing hot-lines. Management reviews and internal audits are also among the main methods of detection, with 16.5 percent found by internal audit in 2016 and 13.4 percent by management review, according to the ACFE. However, KPMG’s study reported that the same percentage of internal frauds (14 percent) were uncovered by accident as through internal audits. “Accidental detection is a sobering reminder that the controls are ineffective,” it says. The UK anti-fraud organization Cifas says that 47 percent of the 409 internal frauds logged by its 172 member organizations in 2016 were detected via internal controls and audit. It comments: “This is reassuring as it means that the investments made by organizations in these processes and, in some instances, software solutions are providing value. It is also likely that these systems are at least partially responsible for the lower levels of recorded internal fraud,” as reported by Cifas for the year.

Employee Monitoring

E

All systems designed to prevent internal fraud depend on employee monitoring, whether through controls that require staff to have certain actions validated by colleagues, or using technology that observes and records each individual's activities on the bank's IT systems and flags any behavior that is suspicious or unusual. Monitoring is an essential part of modern anti-fraud systems because historical data on individuals' behavior must be gathered to allow the creation of profiles against which future behavior can be compared to detect unusual or suspicious activity. Employee monitoring is permitted by law in most jurisdictions, although organizations must disclose to their staff that monitoring is taking place and they may be required by law to carry out an impact assessment before it can be implemented. Covert monitoring is normally permitted only in very limited circumstances involving the investigation and detection of crimes. Making staff aware that their use of the organization's IT systems will be monitored is likely to deter many potential cases of internal fraud. Acceptance of the employer's right to monitor staff and its monitoring policies will usually form part of the employment contract.



F

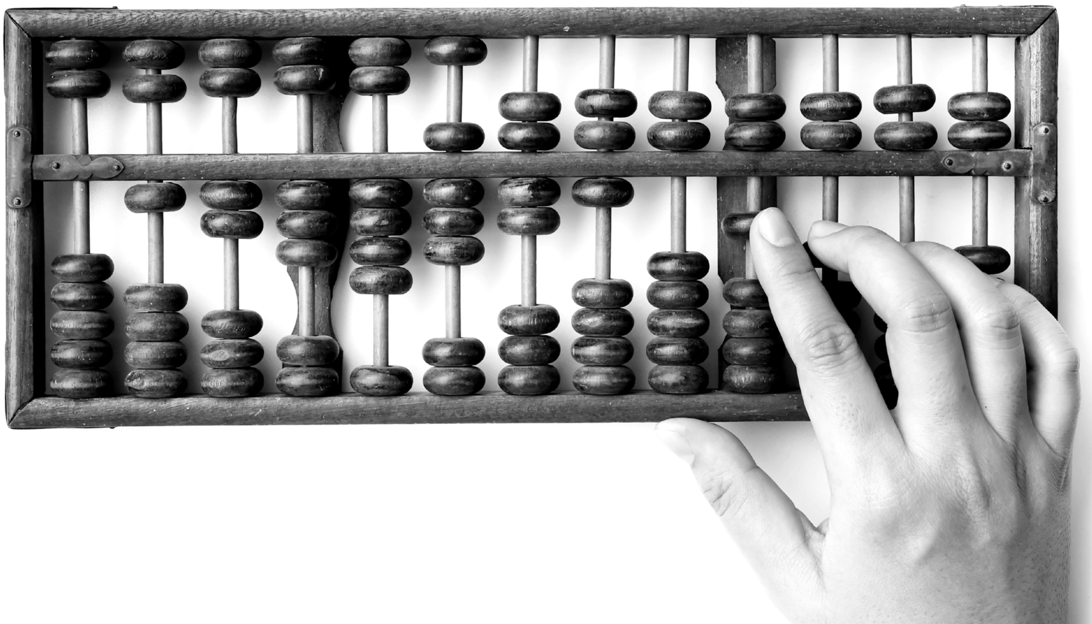
Four Eyes Principle

The Four Eyes Principle is a long-established banking practice that requires staff to obtain validation from a colleague for certain actions, such as payments above a specified amount. This practice is a vital part of the so-called First Line of Defense controls that banks put in place to prevent internal fraud, but even when this control is coded into the bank's systems it has been shown to be vulnerable to abuse. It is obviously possible for staff to collude and so circumvent the Four Eyes Principle, but internal fraudsters may also be able to evade this control by stealing a colleague's system credentials and signing in under their identity to validate a fraudulent transaction. Staff who leave their session open while away from their desk leave the bank vulnerable to this kind of attack. Similarly, bank staff with know-ledge of back-office policies may know the transaction size that triggers the requirement for a second person to validate it, and may therefore attempt a series of smaller payments below the trigger level. Modern anti-fraud systems can flag cases of this nature by employing cumulative payment controls that detect multiple small payments below the Four Eyes limit. They can also flag instances where two members of staff sign on to the system from the same machine in quick succession, indicating possible use of stolen credentials to authorize a transaction.

G

General Ledger

Access to the general ledger and suspense accounts used to hold funds temporarily, such as loans that are being processed or transfers of funds from one department to another, brings major opportunities for internal fraudsters. Staff with knowledge of suspense accounts or the ability to create and update entries can potentially transfer funds, for example as payments to fictitious suppliers, and cover their tracks. Similarly, cases have come to light of staff in private banks using funds taken from suspense accounts to hide losses in clients' investment portfolios and so avoid having to disclose such losses to the customer. Effective technology-led monitoring of staff who have access to the general ledger and suspense accounts is therefore vital to ensure that unusual patterns of behavior are detected immediately and flagged.



H

Holiday

> “
>
> **Instances of weekend working should be monitored carefully via the bank’s card-access management system**

Banks should always monitor staff who do not take all the holiday to which they are entitled. Fraudsters frequently avoid spending time away from the office because their activities require constant management and may come to light if someone else takes on their duties while they are away. Jérôme Kerviel, the trader who brought French investment bank Société Générale close to collapse in March 2008, had not taken a day off in eight months before his unauthorized positions were discovered, according to reports at the time. His activities resulted in a loss of €4.9bn. Following the SocGen case, the UK’s financial regulator recommended that banks insist all staff take a two-week holiday every year. Members of staff working at weekends are another possible sign of trouble that should prompt investigation. Instances of weekend working should be monitored carefully via the bank’s card-access management system.

I

Internal Audit

Internal audit represents the final, Third Line of Defense in the Basel Committee's regulatory framework for managing operational risk within banks. The Third Line of Defense supplements controls that are coded into the core banking systems used by front-office staff and specialist risk-management and compliance functions carried out by the middle and back offices. Many banks continue to rely on a largely manual Second Line of Defense in areas such as risk management and compliance, which is unable to provide comprehensive monitoring of transactions. As a result, they find that most cases of internal fraud are discovered by the internal auditors who make up the Third Line of Defense. However, although internal audit is a critical element of the bank's risk-management governance, reporting to the board rather than the executive management, internal auditors usually focus on specific areas of the bank's operations each year, rather than scrutinizing every part of the operation annually. As a result, auditors tend to detect cases of internal fraud only months or even years after the offenses have taken place. Today, banks are concentrating more on digitalizing their First and Second Lines of Defense, using modern anti-fraud systems that can flag suspect behavior through profiling and machine learning as well as breaches of rule-based controls.

J

Justice

The 2016 *Report to the Nations* by the Association of Chartered Fraud Examiners (ACFE) states that 40.7 percent of internal frauds are never reported to the authorities, mainly to avoid reputational damage to the organization in question. However, despite the widespread reluctance to report internal frauds, bank staff regularly face justice in such cases. In 2017, four members of staff from a British bank were jailed along with three external accomplices for a total of 38 years after passing on the details of dormant accounts holding large balances. In July 2017, a bank teller in the US was charged after stealing $185,000 from a homeless customer who had brought in a sack of cash to deposit in an existing account with the bank. However, in some emerging markets, weaknesses in the prosecution system have meant that cases of internal fraud are not brought before the courts or fail due to lack of evidence, leaving perpetrators free to apply for a job at another bank. Blacklists are often used to weed out suspected fraudsters.

K

Key Types of Fraud

Transaction Reversal by Tellers

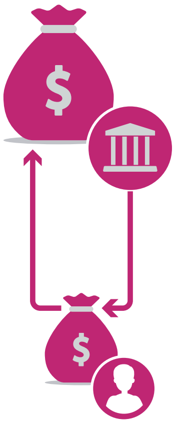
A problem in emerging markets, where bank staff reverse deposit transactions after the customer has left the branch and steal their money.

Account Manipulation

Where employees remove charges or change interest rates on loans or credit limits, usually to benefit their family or friends.

Loan Applications

Another common tactic is to steal a customer's personal details and use them to apply for loans or credit cards in the customer's name.



Hiding Losses

Losses on a private banking customer's investment portfolio can be hidden by temporarily taking money from the bank's suspense account – used to hold funds pending reconciliation and allocation to the final account – and transferring them into the customer's portfolio account to increase the balance. After the client meeting, the funds are transferred back to the suspense account. Anti-fraud technology flags unusual behavior around suspense accounts.

Four Eyes Violation in Private Banking

A transaction on behalf of a client is entered in the private bank's portfolio-management system. It is then screened by compliance before being validated. However, this validation might take place hours or even days later, and the transaction may be validated in a different banking system, by a different employee in a separate department. If the bank does not have a control in place to check that the user profile of the person who originally entered the transaction is different from the user who later validates it in a different banking system, there is a risk that the same employee could both create and authorize a fraudulent transaction. However, even where such a control exists, a fraudster can get round it by signing in with another employee's user credentials to validate the rogue transaction. This illustrates why rules-based controls are not enough on their own. Banks also need user-profiling software to detect suspicious behavior – a user signing in from an unusual machine or appearing to sign in when they are not in the building, suggesting someone else is using their login details.

Internal Collusion

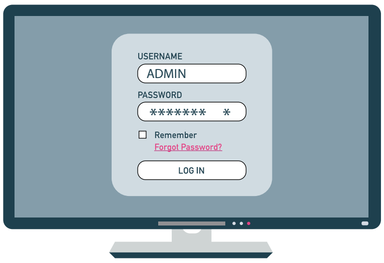
Normally occurs where two or more employees must work together to circumvent static controls, for example by approving fraudulent payments in violation of the Four Eyes Rule.

Data Theft

Bank customers' data, including pin numbers and account details, are vulnerable to theft by members of staff. This information can then be sold on the black market.

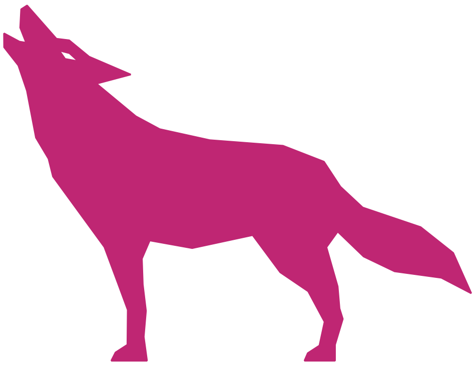
IT Changes at the Back End

Staff with IT administrator privileges can play a key role in internal frauds, for example by granting administrator rights to non-IT staff for just long enough to allow them to approve a fraudulent transaction.



L

Lone Wolves and Large Groups



Internal frauds are committed both by lone wolves and large groups, and the two types show important differences. Frauds involving several conspirators make up at least half of the global total and around 75 percent of Latin American, African and Middle Eastern cases, research has found. Fraudsters collude because they need help from others to circumvent controls or because they lack crucial information. Studies show that solo frauds tend to be carried out by younger and more junior employees, while those who collude are typically more senior and have longer employment histories at the company. They also result in bigger financial losses. About a third of frauds involving collusion result in losses of more than $1m, twice the proportion of solo frauds costing the same. The ACFE reports that frauds involving five or more people resulted in a median loss of $633,000 in 2016, more than twice the median figure for frauds involving four people. There were also big differences in the most common ways in which lone wolves and large groups were detected. Solo frauds tend to be discovered by accident or as a result of a management review or internal audit. Frauds involving collusion are twice as likely as solo crimes to be exposed by a tip-off or complaint to the company.

Machine Learning

M

Machine learning represents the next frontier for anti-fraud systems, acting as a third level of security. These advanced computing techniques build on the foundation of static rule-based controls (qv) and behavioral profiling (qv) to give a more accurate and sensitive set of fraud-detection tools. The application of machine learning in anti-fraud systems involves using large volumes of historical data to train algorithms, so that they progressively learn to identify anomalies among the mass of legitimate transactions. Machine learning-based anti-fraud systems draw on five main approaches. These are:

- **Peer-group analysis:** This technique enhances profiling by enabling the system to create profiles for sub-groups of customers, such as people who go on holiday in summer. This allows it to compare the profiles of individual members of the group against the whole to detect unusual behavior or transactions.

- **Markov models:** These analyze the way in which users progress through a series of steps, for example in using an e-banking platform or an internal workflow. It allows each user's progress to be compared with the normal pattern to highlight unusual behavior.

- **Random forests:** Decision trees classify information based on a series of questions that lead to a range of possible outcomes. Random forests are collections of decision trees that allow more nuanced and accurate classification of anomalous activity than a single, more linear one.

- **Neural networks:** These are software systems loosely based on the structure of the human brain that are trained with large bodies of historical data to flag patterns that indicate certain features or activities. If the network's decision is wrong, the connections between its artificial "neurons" change to take the error into account and alter subsequent decisions.

- **Entity-link analysis:** Also known as relationship discovery, this employs graph-analysis techniques to identify relationships between people inside and outside the bank in order to detect collusion. For example, if several employees send many small payments to a series of accounts outside the bank – that individually would not trigger an internal control – this technique can enable the bank to establish the relationship between the different conspirators.

N

Negligence

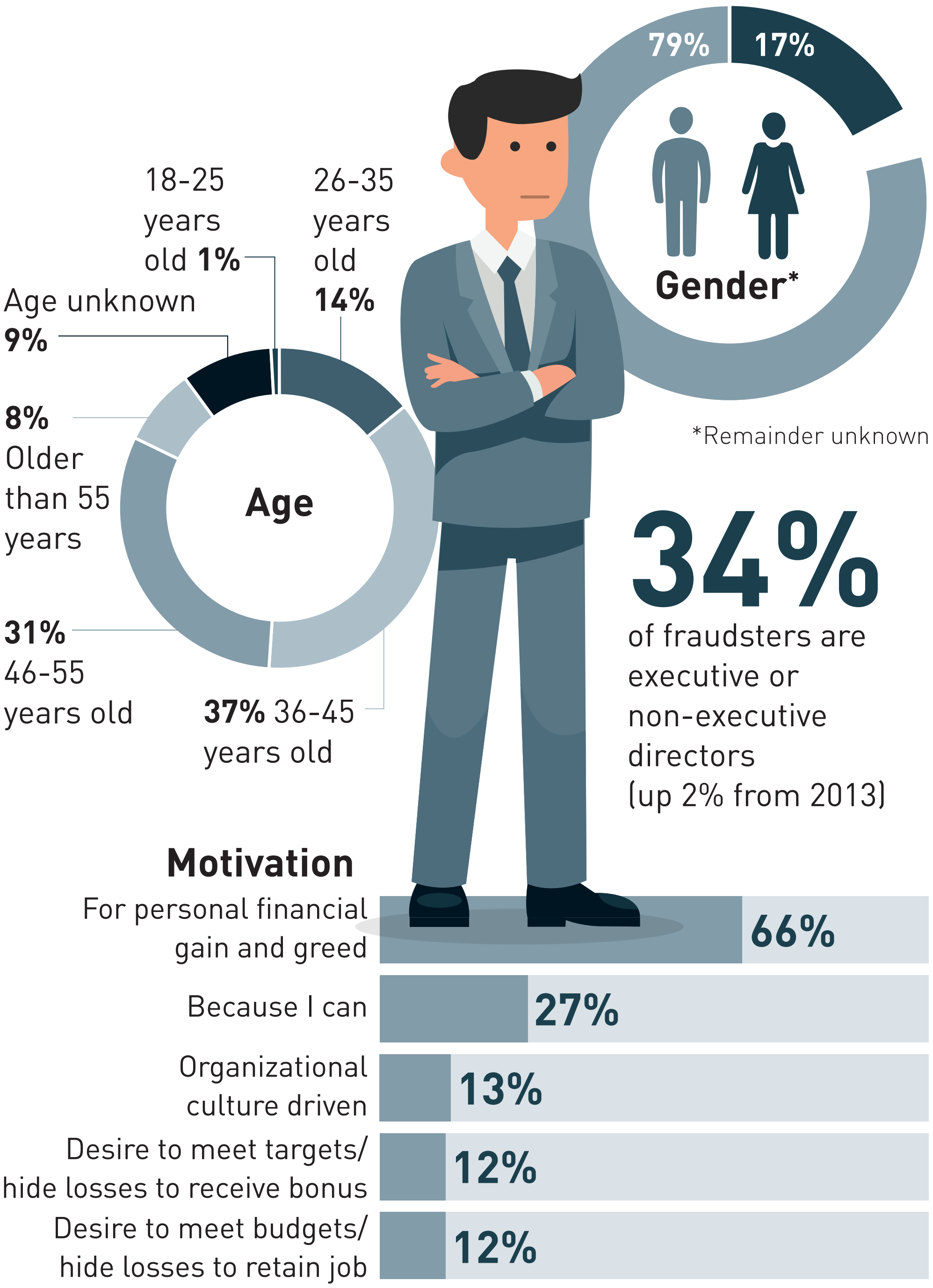
As fraud-detection technology improves over the next few years, thanks to advanced computing techniques, the risk increases that institutions that choose not to implement modern systems will leave themselves increasingly open to accusations of negligence if they fall victim to fraud. *Global Profiles of the Fraudster 2016* found that "an increasing number of organizations are introducing data analytic solutions to search for unusual transactions... But data analytics does not appear to be fully deployed by companies." Just 3 percent of frauds were detected using "proactive data analytics", compared with 24 percent of technology-enabled frauds that were uncovered by accident. In its 2016 report, for the first time, the ACFE asked organizations that had fallen victim to fraud whether they had been fined as a result. Some 8.4 percent of victim organizations had been fined: in 31 percent of cases, the fine was between $100,000 and $1m; and in 22 percent of cases it was greater than $1m. Organizations that suffer fraud – as well as fraudsters – face the risk of official penalties for their role in any losses.

Outsiders

O

Statistics on frauds that involve outsiders colluding with staff vary widely between different research sources: some report that frauds involving purely internal collusion typically result in greater losses than frauds that involve both outsiders and insiders; others find that there is little difference in impact between the two types. In spite of these variations in research findings, organizations need fraud-detection systems that can "look both ways", inside and outside the business, and they must be alert to the risk that a lone internal fraudster may have a large group of accomplices on the outside. The ability to identify connections and relationships between insiders and individuals outside the company is a key anti-fraud measure, often known as entity-link analysis or relationship discovery. Visualization of relationship networks (qv) allows these patterns of strong and weak links between employees and outsiders to be displayed graphically, greatly aiding detection.

P Profile of an Internal Fraudster



34% of fraudsters are executive or non-executive directors (up 2% from 2013)

Source: Global Profiles of the Fraudster, KPMG International, 2016

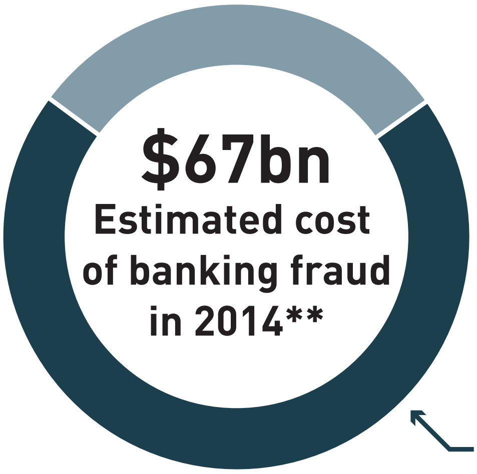
Q Quantum of Fraud

The Association of Chartered Fraud Examiners' 2016 Report to the Nations revealed that...

The typical organization loses 5 percent of its revenue in any given year as a result of internal fraud*.

Applying this to the 2014 estimated Gross World Product results in a total loss to fraud around the globe of up to:

$3.7 trillion



$67bn
Estimated cost of banking fraud in 2014**

70% of this fraud is internal

16.8%
Of all global losses due to internal fraud were in banking and financial services – the highest across all industries

40.7%
The percentage of cases in which the victim organizations decided not to refer the fraud to law enforcement – fear of bad publicity being the most cited reason

Sources: *Applying this percentage to the 2014 estimated Gross World Product of $74.16 trillion
**Association of Chartered Fraud Examiners 2014 Report to the Nations on Occupational Fraud

R

Real Time

The ability to monitor transactions and flag suspicious activity in real time is an extremely important advance in anti-fraud technology that has made these systems much more effective. Until recently, even the most advanced systems operated with a slight lag. However, this is no longer necessary and the leading anti-fraud systems now operate in real time, extracting data from the core banking system and analyzing it instantly. This allows suspicious transactions to be blocked before they can complete, greatly reducing the likelihood that money will be lost due to fraud, as well as minimizing burdens on the core banking system that could degrade its performance.

Static Rule-Based Controls

S

Static rule-based controls represent the First Line of Defense for any software-based anti-fraud strategy. Such rules are hard-coded into the core banking system to enforce anti-fraud measures. They include the segregation of duties, the validation of transactions above a specified value by a second pair of eyes and checks to ensure that the user who validates a transaction has not had their profile changed to enable them to do so. Rule-based systems are important, but do not provide sufficient protection on their own. Determined fraudsters can circumvent controls that require transactions to be independently validated by stealing another user's credentials, for example. A fraud committed in this way will appear to comply with a system of static rule-based controls; instead, behavioral profiling (qv) would be required to detect such activity. A further problem with rule-based controls is that in order to design them, compliance staff must know how the fraud will be executed. Controls will not necessarily help the organization when the mechanism is not known in advance. To do this, other anti-fraud techniques based on machine learning (qv) must be overlaid on the framework of controls.

T

True and False Positives

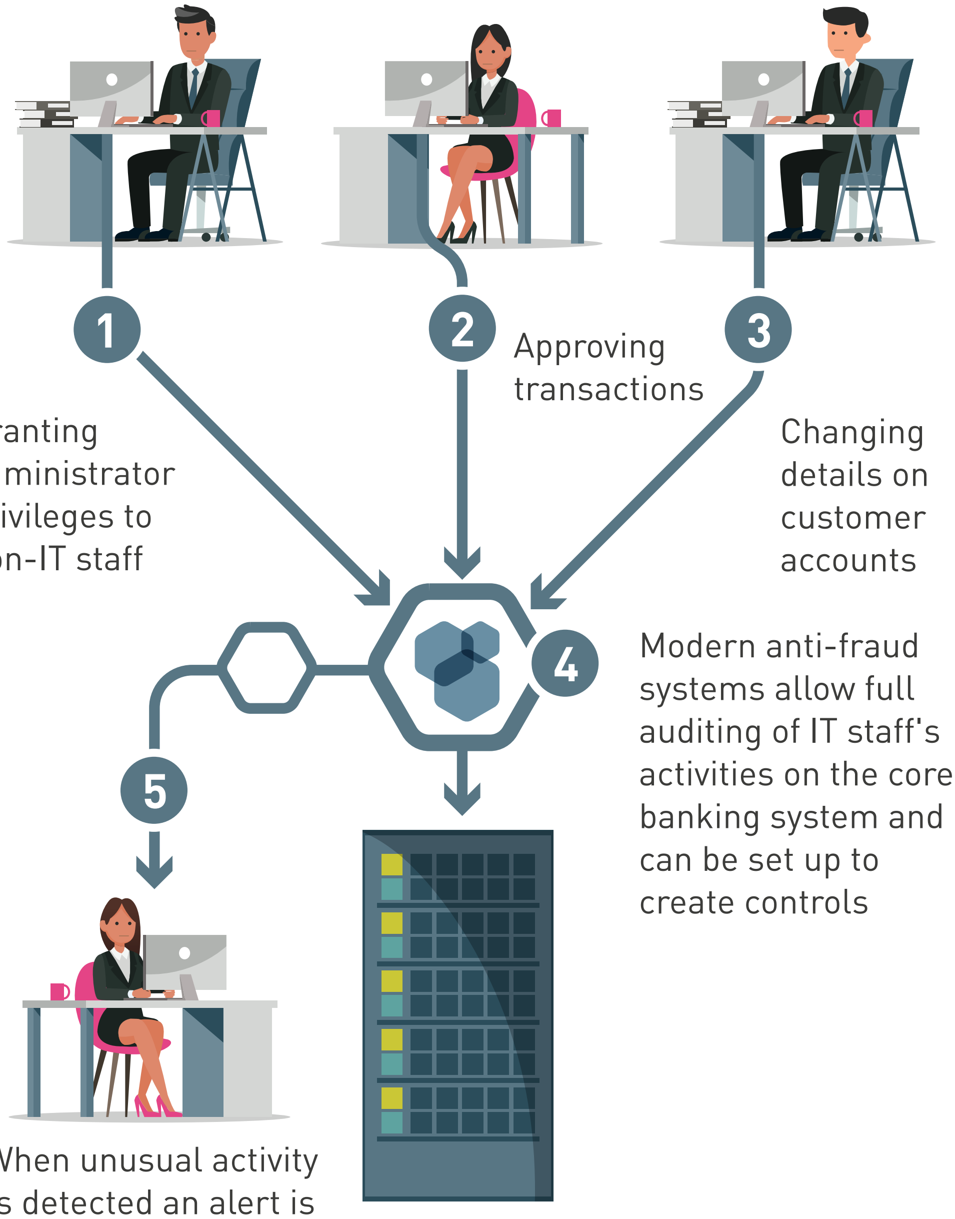
Technology-based anti-fraud systems, whether they depend on static rules or behavioral profiling, produce both true and false positives. Systems that use profiling are based on probabilistic models; each transaction is scored against the risk parameters built into the model and those that score above a certain threshold are flagged for investigation, their score reflecting the probability that they are fraudulent. The challenge that banks face in implementing them is to balance the sensitivity of the system – and therefore its ability to identify frauds – against the inconvenience that customers suffer when their legitimate transactions are blocked. Research and development work by anti-fraud software providers today focus on refining the tools to make them more sensitive and more precise, reducing the number of false positives that the system generates and increasing the true positives. A number of machine-learning (qv) applications are now being developed to supplement the existing controls and profile-based techniques currently used to detect fraud. NetGuardians' application of machine learning-based anti-fraud technology has been found to reduce the number of false positives by 80 percent.

> “
>
> **Research and development work by anti-fraud software providers today focus on refining the tools to make them more sensitive and more precise, reducing the number of false positives**

U User Access Monitoring

Privileged IT users working on the core banking system can be very difficult to monitor without specialist software tools.

They have a lot of opportunity to make changes on the system that could lead to frauds, such as:



1 Granting administrator privileges to non-IT staff

2 Approving transactions

3 Changing details on customer accounts

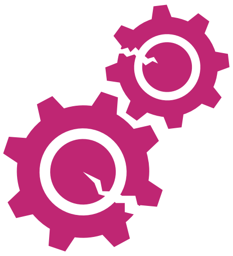
4 Modern anti-fraud systems allow full auditing of IT staff's activities on the core banking system and can be set up to create controls

5 When unusual activity is detected an alert is sent to the risk/ compliance officer

V Visualization of Relationship Networks

Advanced anti-fraud software can combine data taken from multiple sources about individuals and organizations, and plot the links between them. This becomes a much more powerful tool when the data map is then visualized so that investigators can see the links that have been detected, for example between individuals within an organization, and between insiders and other associates outside the organization. This helps in identifying more complex fraud networks that rely on collusion between employees and outsiders.

W



Weak Controls

Weak controls are the single most important factor behind internal fraud and play a central role in more than 70 percent of internal frauds uncovered in Europe and more than 60 percent globally, according to recent research. Weak controls therefore represent a major management challenge for financial-services firms, as well as an opportunity to benefit from improved practices. Poorly designed controls and/or a weak workplace culture of compliance create the most attractive opportunities for internal fraudsters, and the problem appears to be getting worse. Researchers found that in 2013, 18 percent of the fraudsters it interviewed committed their offense because such an opportunity presented itself. By 2016, that proportion had risen to 27 percent. Weak controls are a serious problem, not only because they make it more probable that a company will be targeted by internal fraudsters, but also because regulators are more likely to impose fines and other sanctions on organizations that suffer frauds that can be attributed to negligence (qv) in this area.

X

XXIst Century Fraud Solution

Technology-led systems capable of analyzing every transaction that takes place in real time represent the best 21st-century fraud solution. They already offer far greater protection than the manual processes long depended on by financial institutions and their effectiveness will be refined over the coming years as advanced computing techniques begin to supplement the main existing approaches based on behavioral profiling (qv). The result is greater accuracy and an improving ratio of false positives. NetGuardians' anti-fraud solution uses machine learning to reduce the proportion of false positive flags by 80 percent. This leads to a 93 percent reduction in the time spent dealing with them and significantly increases a bank's operational efficiency. The *Report to the Nations* is clear on the benefits of adopting technology-based anti-fraud systems: "The 36.7 percent of victim organizations using proactive data-monitoring and analysis… suffered losses that were 54 percent lower and detected the frauds in half the time compared to organizations that did not use this technique."

Y

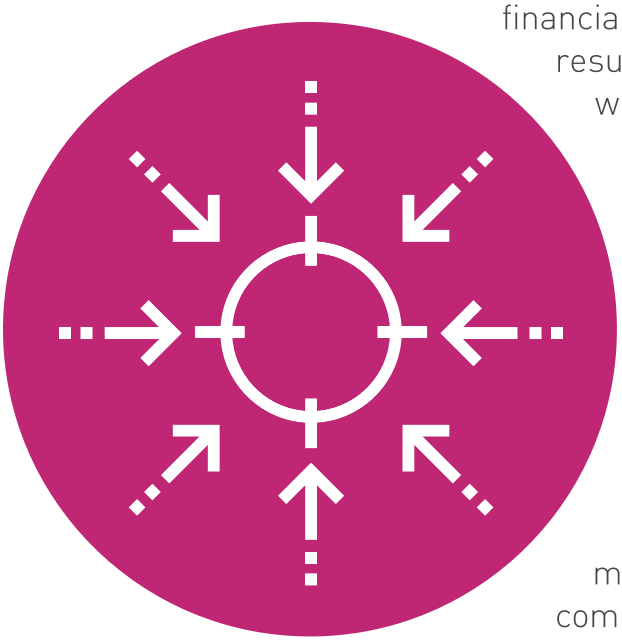
Youth

Studies show that up to 60 percent of perpetrators in technology-enabled frauds are aged between 26 and 45

Although most surveys indicate that around two-thirds of internal fraudsters tend to be aged between 36 and 55, youth is an important factor in a significant number of cases. For example, in February 2017, a 23-year-old former UK bank employee received a two-year suspended jail sentence after using a customer's details to open an account and obtain a loan in his name, £78,000 of which was withdrawn from the bogus account. The customer raised the alarm after receiving paperwork for the fraudulent loan through the post. The UK anti-fraud organization Cifas found that among the 409 cases of internal fraud reported by its members in 2016, 53 percent of the perpetrators were aged between 21 and 30, a far higher proportion than in larger, international studies. There is also evidence that younger employees are more likely than older fraudsters to use technology to perpetrate a fraud. Studies show that up to 60 percent of perpetrators in technology-enabled frauds are aged between 26 and 45 – a much higher concentration of younger staff than in cases that do not depend on technology. The signs are that as younger, more tech-savvy employees climb through the ranks, the incidence of technology-related fraud is likely to rise. Tech-enabled frauds are also much more likely to be discovered by accident (24 percent) than overall cases of internal fraud (11 percent), suggesting that controls are more easily evaded in cases where technology is exploited.

Z Zoom In

FinTech companies develop technology to target specific activities or financial services, enabling these providers to zoom in on a particular area and find new and better ways to address it. As the financial-services industry digitalizes and the technology tools grow steadily more complex, access to market-leading tech expertise is becoming more critical than ever for banks and financial-services groups. As a result, banks are increasingly working with specialist FinTech providers, rather than generalist IT companies, to gain access to the most advanced specialist solutions and to benefit from the speed and agility of these niche providers. Thanks to their focus on specialized market niches, FinTech companies understand their clients' needs and can offer a highly responsive service. They also tend to be closer to the emerging fraud techniques than less specialized service providers. Technology is playing an ever-growing role in internal fraud. Banks have no choice but to meet that threat with the leading-edge anti-fraud systems that specialist FinTech providers are bringing to market.



NetGuardians

For further information on how to prevent internal banking fraud 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. Its 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.