RECLAIM YOUR POWER IN THE BATTLE AGAINST FRAUD

THE HUMAN FACTOR

FIS WHITE PAPER

Fraudsters know the easiest way to breach an organization's defenses is to target its people. Furthermore, 70 percent[1] of reported economic crimes are committed by internal actors, making internal fraud the biggest risk. In this white paper, we consider the main types of fraud all financial institutions must be aware of and how to combat them.

Social Engineering – The Sinister Art of Manipulation

With 79 percent[2] of attacks successfully misappropriating funds, social engineering is one of the biggest crime threats for banks and other financial institutions. Attacks rely on human error, so they are hard to predict. Social engineering attacks may progress in one or more steps and regularly defeat all the lower-level IT security measures. Many attacks go undetected for long periods.

Although social engineering requires skill, it is much simpler to commit than many other frauds, such as hacking into a bank's computer system. C-level executives are often the target of social engineering attacks because they have "the keys to the kingdom" in the form of unchallenged authority and privileged access to sensitive information.

Social engineering involves stealing bits of an individual's persona to build a complete identity jigsaw puzzle, using public sources like social media profiles, and manipulating individuals into divulging pieces of information that eventually lead to a complete picture of target individuals.

[1]Clari5, The Threat Within. Spotting and Arresting Insider Fraud, April 2019
[2]CyberEdge, 2017 Cyberthreat Defense Report

Types of social engineering fraud:

- **Invoice fraud** is a common way for fraudsters to take money and it can easily go unnoticed as being fraudulent. When it occurs, there can be a dispute about whether there was contributory negligence.

- **Business email compromise fraud** is the fastest-growing internet financial crime, nearly $1.3 billion[3] in the U.S. during 2018. Typically, this involves a hoax email, which fraudulently represents a senior colleague or a customer. The email usually issues instructions such as approving a wire payment or releasing client data.

- **Phishing** scams account for over 90 percent of data breaches and are growing at more than 65 percent[4] each year. Many phishing attacks target bank employees, attempting to obtain sensitive information, such as usernames and passwords. The ultimate goal is to trick bank employees to click on links or open attachments that redirect them to fake websites. There they are encouraged to share login credentials and other personal information.

- **SMiShing** (SMS phishing) tricks a user into downloading a "Trojan horse" onto a cellular phone or other mobile device. In effect, the user has handed over access to their phone without realizing it. The installed piece of malware might steal phone numbers, banking data or spread the virus to all contacts on the phone. SMiShing is a new channel for criminals to exploit. With the growth in mobile banking and payments, the incentives for criminals are increasing exponentially. As people become accustomed to automated texts, it becomes easier to exploit that familiarity.

[3,4] *FBI, Internet Crime Report 2018*

Identity Theft and Account Takeover

Identity theft can take many forms, but account takeover (ATO) is the most prevalent. Fraudsters take over existing accounts to transfer funds to new destination or "mule" accounts at other institutions. This type of fraud has been around for decades, but attacks are mushrooming with the growth of the digital economy. As more elements of consumers' identities have appeared on vulnerable databases, fraudsters have sold complete packages of identity information needed to open a fraudulent account. This has propelled ATO fraud to an industrial scale worldwide.

ATO takes many forms but the biggest surge has been in online fraud. The growth in mobile banking and real-time payments has increased banking convenience for customers but also increased opportunities for fraudsters. Funds can be routed to mule accounts in real time and apps have been a catalyst to ATO attacks.

The most striking characteristic of the recent shift in ATO tactics is its ambitious scale. Many banks have experienced a ten-fold[5] increase in incident rates within the last year. The industrialization of ATO shows that fraudsters are well prepared on both sides of the payment. On the victim side, the fraudsters need credentials and an automated way of compromising the victim's account. On the mule side, they need a list of accounts to receive the stolen funds.

Internal Fraud – The Enemies Within

Banking is experiencing immense technical disruption but it's still fundamentally a people business. As ambassadors of a bank's brand and advocates of its intangible services, a bank's people represent all that's good about the organization. Internal fraud is a tender subject and many financial institutions don't realize they have an internal fraud problem because they cannot detect it. Yet it is estimated that about 5 percent[6] of an organization's revenue is lost to fraud. A recent report[7] finds the average occupational fraud scheme goes undetected for 18 months.

As already mentioned, internal fraud has become a huge global challenge. The prospect of financial loss can be significant, but this is far outweighed by the risk to reputation and brand. In the United Kingdom (U.K.), a few shocking market abuse and trading scandals, particularly the London Interbank Offered Rate (LIBOR) scandal, caused immeasurable damage to some major bank brands and to the industry. In the last decade, the top five banks in the U.K. have been fined over £25 billion by various regulatory authorities. These scandals have also resulted in a tighter regulatory framework that increases the cost of business for all.

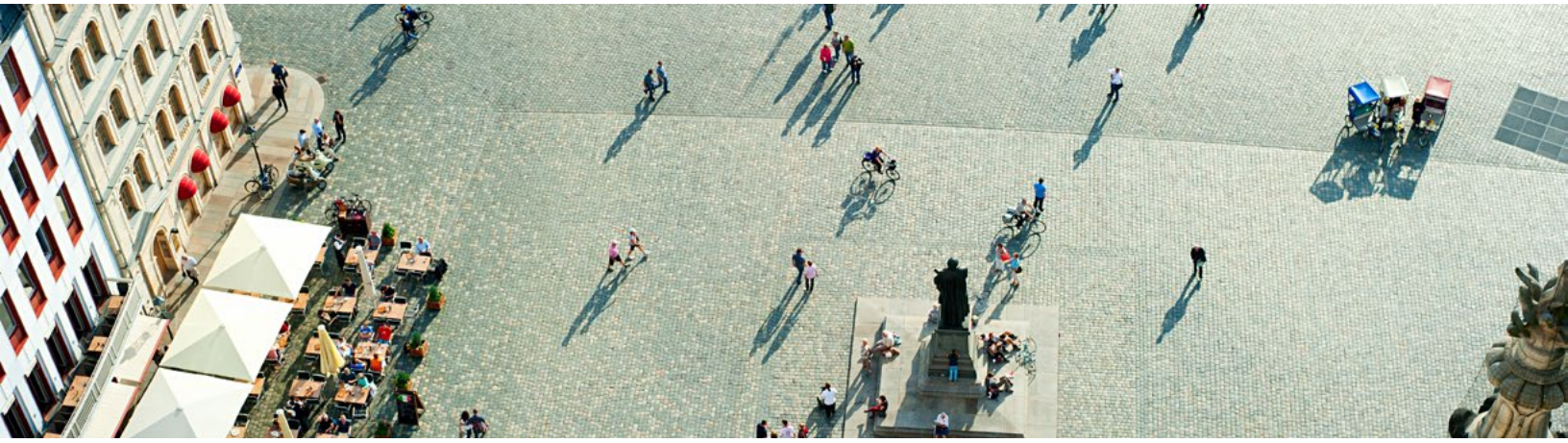
Despite a growing body of regulation, many organizations struggle to tackle the problem of internal fraud. All too often, fraud prevention and detection measures focus on keeping external fraudsters out. Rules-based solutions may be incapable of detecting internal fraud or can be easily circumvented. A more sophisticated approach to fraud detection is needed to deliver an integrated solution that can consolidate and analyze data in different formats from multiple sources, as internal fraud can take many forms.

[5]Aite Group, Trends in Account Takeover Fraud for 2019 and Beyond
[6,7]Association of Certified Fraud Examiners' (ACFE) Report to the Nations on Occupational Fraud and Abuse

General Ledger Fraud

Sadly, it's often long-term employees who most often abuse positions of trust and privileged access to bank systems and information. The typical internal fraudster has been employed for over 10 years and is familiar with the systems and their shortcomings.[8] For example, certain insiders may have exclusive access to accounts payable or suspense accounts that are used to record loans in process or currency in transit. This can make it easy for experienced employees to move funds between accounts or issue payments to external companies, which may be bogus. Over time, money can be funneled from general ledger accounts to mule accounts and can easily go unnoticed for a long time. Examples include a bank employee who was convicted of stealing more than $4 million accounts over a period of 8 years and concealing the money in the general ledger.[9]

Tackling general ledger fraud requires the right mix of processes and systems. By segregating duties, no employee will be able to set up accounts and effect funds transfers. Technology can improve oversight through automated monitoring of journal entries while checking for irregularities.



Collusion with Outsiders

The most harmful crimes tend to involve collusion with outsiders. Many ATO fraud schemes involve bank staff in collusion with outsiders. For example, a member of staff may open a legitimate account for a customer and then open an online account to drain funds from the account. Alternatively, an employee may grant a loan to a fraudster posing as a legitimate customer. Subsequently, the employee steals the money and makes it look like the customer has absconded with the funds.

The number of ways for insiders to collude with outsiders is limited only by the imagination of the fraudster. All banks need a framework for fraud detection.

[8]Global Banking and Finance Review, April 2015
[9]*Banking Exchange, 4 internal frauds and how to spot them*

A Framework for Fraud Detection

- **A strong system of internal controls and auditing is critical.** Distributed accountability reduces the potential for identity theft and ATO. Close monitoring is crucial to identify irregularities early and also to act as a deterrent. When staff know they are being monitored, they are less likely to commit crime.
- **Access to customer information must also be tightly controlled.** Permission should only be granted where it is necessary to perform a clearly defined job. Technology can monitor all systems logins to establish patterns and spot anomalies, such as after-hours logins. Although it's useful to have an audit trail of systems access, real-time technology can offer a step-change improvement in fraud prevention and detection.
- **Cross-channel monitoring to protect multiple portfolios.** This is especially important when customers hold products in different channels. By detecting events on one channel and using link analysis to investigate activity on other products held by the consumer, you will have the ability to quickly ascertain whether an ATO is broader than the original alert.
- **Regular training to make staff more vigilant.** Staff must be aware of their vulnerabilities, especially when they are socially engineered to divulge information or enact payments on behalf of fraudsters. Staff are always susceptible to fraud, but they are also the first line of defense.

To discover more ways to prevent fraud, read our tip sheet here.

Don't react. Outsmart.

When you can predict financial crimes in every channel, you regain power over fraudsters. With highly scalable machine learning and AI capabilities, FIS Memento spots fraudulent transactions across your entire firm in real time and predicts new threats. Plus, you gain all the cross-channel tools your staff needs to efficiently and holistically manage any threat. It's just one of the reasons FIS has ranked No. 1 on the RiskTech100 list four years running.

TO LEARN MORE ABOUT FIS' INNOVATIVE FINANCIAL CRIME MANAGEMENT SOLUTIONS, click here OR CONTACT getinfo@fisglobal.com.