The forensic professional's perspective on fraud and fraud detection

Received (in revised form) 12th May, 2021

Timothy P. Hedley*
Senior Adviser at K2 Integrity, Fordham University, USA

Richard H. Girgenti**
Vice-Chairman, K2 Integrity, USA

Timothy Hedley, *PhD, is a Certified Public Accountant, Certified in Financial Forensics and a Certified Fraud Examiner. He has over 25 years of experience providing clients with a wide range of forensic services by assisting with the prevention, detection and response to fraud, misconduct and other integrity risks. He was a partner in the forensic practice at KPMG LLP, serving as Global Lead for the firm's Fraud Risk Management service offerings. He has served on the faculty at several universities, including New York University and the State University of New York at Albany. Currently, he serves on the faculty at Fordham University, where he teaches Business Risk in a Global, Digital Economy. He is also a board member and treasurer of the Connecticut Society of CPAs. He frequently presents to corporations, professional organisations and academic institutions on a variety of topics, including fraud, misconduct and compliance risks.*

Richard H. Girgenti *is an attorney, risk and compliance consultant and Certified Fraud Examiner. He graduated from Georgetown Law School and formerly served as a prosecutor in the Manhattan District Attorney's Office. He also served as the NYS Director and Commissioner of Criminal Justice Services and a Board Director and leader of KPMG, LLP's Forensic Advisory Services and member of the Global Forensic Advisory Board. He currently serves as the Vice-Chairman of K2 FIN, an investigations, compliance and risk advisory firm, the Senior Counsel to Compliance Systems Legal Group (CSLG), a boutique law firm that focuses exclusively on corporate compliance, ethics and governance and the CEO and Founder of IDPL, a risk consulting and executive coaching firm. He is a frequently called upon author and lecturer. Rich and Tim are coauthors of the books* Managing the Risk of Fraud and Misconduct: Meeting the Challenges of a Global, Regulated, and Digital Environment *(2011) and* The New Era of Regulatory Enforcement: A Comprehensive Guide for Raising the Bar to Manage Risk *(2016). Both were published by McGraw Hill.*

Timothy P. Hedley

Richard H. Girgenti

Abstract

As banks and other financial institutions become increasingly complex and rely more heavily on remote and online services, they face an ongoing and ever-changing challenge presented by fraudsters who also have devised increasingly sophisticated methods to commit fraud. An effective compliance and fraud risk management programme must incorporate better and more sophisticated ways to meet the challenge of fraud. To this end, most organisations are increasingly turning to data analytics to help devise better methods to prevent and detect fraudulent activities. At the core of this effort to develop technology solutions to combat fraud are the skills, experience and competencies of forensic professionals. It is essential that any fraud risk management programme rely upon and leverages the diverse expertise of forensic professionals who will have the industry expertise, understanding of regulatory mandates, knowledge of fraud and their red flags and the various schemes devised to commit fraud. These professionals must also possess the investigative and forensic accounting acumen

**441 E. Fordham Road,*
Bronx, NY 10458,
USA
Tel: +1 917-743-1047;
E-mail: thedley@fordham.edu

***845 Third Ave,*
New York, NY 10022,
USA
Tel: +1 914 960-7766;
E-mail: rgirgenti@k2integrity.com

Journal of Financial Compliance
Vol. 5, No. 1 2021, pp. 85–93

2398-8053

to detect fraud and the data analytic competency to help programmers and data scientists devise the rules and algorithms required to detect fraud and, ultimately, the ability to identify and investigate the data anomalies that will result and require further analysis. This paper discusses the unique perspective and expertise of the forensic professional, the nature of fraud, the forensic fraud detection process, sample banking fraud schemes and how the forensic competencies inform and enhance the power of data analytic processes from rules-based to artificial intelligence (AI) and predictive analytics.

Keywords: fraud, forensic, scheme, analytic, risk factors, red flags

INTRODUCTION

The forensic professional has held an ever-increasingly important role in mitigating fraud risks at financial institutions. This paper aims to help the reader understand, in context, the forensic professional's perspectives, skills and methods. To help reinforce this understanding, we provide the reader with examples of the forensic perspective by stepping through a series of fraud scenarios using the forensic fraud detection process. We will start our discussion with the colourful Willie Sutton.

Willie Sutton was the most notorious American bank robber in the first half of the 20th century. An often-repeated but perhaps apocryphal story was when asked by a reporter why he robbed banks, he replied, 'Because that's where the money is'.[1] Before Sutton was robbing banks and up to the present time, banking frauds have been taking place because that is where the money is. In the modern digital era of technology, online banking, the internet and cybercrime, the schemes have become ever more sophisticated

Frauds in the financial sector today capture headlines that would have staggered the imagination of even the infamous Willie Sutton. For instance, over the last two decades, many of the largest global banks paid enormous fines for manipulating the interest rates at which banks lend to each other (known as London Inter-Bank Offer Rate [LIBOR] for US dollar lending and EURO LIBOR for euro-denominated debt). Wells Fargo engaged in illegal sales practices when aggressive sales practices pressured employees to sell to an astonishing level unwanted or unneeded products to customers.[2]

Further, many banks got themselves caught up in scandals involving fraud and misconduct in packaging subprime mortgage debt that resulted in massive home loan defaults and led to the financial recession in 2008–9. Rogue traders like Jerome Kerviel, who lost SocGen £3.7bn, and Nick Leeson of Barings, who brought down one of the most storied British banks losing £827m in unauthorised trading, would have been the envy of Willie Sutton.

More recently, Wirecard, a German Fintech company, applied for insolvency, and its top executives were arrested and criminally charged with a variety of frauds. Among these frauds were a series of accounting frauds designed to inflate sales and profits that resulted in nearly €2bn missing or lost due to deception.

When one step past the headlines, the pervasiveness of fraud in the financial sector is even more remarkable. According to the highlights of the 2019 American Bankers Association (ABA) Deposit Account Fraud Survey of 151 institutions of all sizes, losses due to fraud rose to US$2.8bn in 2018, up from US$2.2bn in 2016. Debit card fraud accounted for 44 per cent — or US$1.2bn — of losses in the industry, which slightly decreased from 2016. The study also found that check fraud was on the rise, now making up the majority, and accounted for 47 per cent of fraud losses. Additionally, 9 per cent of the fraud losses were attributable to online banking and other electronic transactions.[3]

As extraordinary as this data is, according to the ABA Survey, attempted frauds against banks reached US$25.1bn in 2018, up from US$19.1bn in 2016 and US$12.9bn in 2014, which was even more noteworthy. Fortunately, banks stopped US$22.3bn in fraud attempts or approximately US$9 out of every US$10 of attempted deposit account fraud.

Corporate regulators and banking regulators have recognised the challenges that fraud presents to the integrity of financial institutions. The result has been a variety of regulatory rules and mandates from, among others, the US Federal Reserve Bank, the Office of the Currency Comptroller and the UK Financial Conduct Authority regarding the responsibility of banks for effective fraud risk management.

In light of increasingly complex fraud schemes and regulatory and enforcement scrutiny, financial institutions have had to enhance their efforts at prevention and detection. In these efforts, it is the skill of forensic professionals that inform the procedures and analytics that are required to identify the patterns of fraud and weaknesses in internal controls. Forensic professionals also provide the scepticism, knowledge and intuition essential for effective fraud risk management.

Forensic professional is not a defined term. There is literature discussing and describing relevant terms, such as forensic accountant, fraud auditor and fraud examiner. Other professional descriptions, such as white-collar investigators, computer programmers and data scientists, also involve forensic-related skills.

For this paper, the authors use the term forensic professional to describe a multidisciplinary fraud specialist. These specialists possess a combination of skills and competencies. These skills include forensic accounting, fraud examination, legal and regulatory expertise, investigative acumen, industry expertise, data analytics, evidence gathering, interviewing expertise, internal control review capabilities, risk management, behavioural science, governance and compliance. Fundamentally, the results and evidence produced by applying these competencies would withstand judicial scrutiny.

BASIC CONCEPTS AND THE NATURE OF FRAUD

Before exploring, by example, the forensic professional's perspective on fraud and fraud detection, we must define some basic concepts.

Fraud

There is no widely accepted single definition of fraud, but we can construct one. A synthesis of commonly held meanings would maintain that it is a form of behaviour, generally held by the courts, as an intentional misrepresentation that was appropriately relied upon by the plaintiff and caused the plaintiff damages. This type of characterisation makes it challenging to manage fraud risk proactively as it requires measuring the harm caused or the unfair gain when considering fraud risk and detection. For our purposes, we define fraud as an intentional deception that drains value from an organisation.[4] This delineation will eliminate the need to quantify fraud loss and focus on fraudulent behaviour's fundamental nature.

There are three broad categories of fraud: asset misappropriations, fraudulent financial reporting and corruption. Asset misappropriations are the embezzlement of cash, the theft of cash or other assets and the misuse or abuse of organisational assets. Fraudulent financial reporting is the intentional misrepresentation of financial information for internal or external reporting purposes or as needed for management decision-making purposes. Finally, corruption is undertaken by persons in positions of authority who abuse their power for their personal gain,

typically as bribes or kickbacks. This paper will limit itself to examples of select asset misappropriation frauds.

It is also essential to recognise that fraud is perpetrated internally, externally or collusively. Employees, management commit internal frauds and third parties retained by the bank and include, for example, financial reporting frauds, deposit transformation frauds, rouge trading and asset quality manipulations. Internal fraudsters take advantage of their knowledge of and access to systems and controls to commit fraud. External fraudsters are individuals with no formal association with the bank and include credit card schemes, account holder impersonation and e-mail phishing. In this context, when fraud is against the financial institution, it is referred to as a first-party fraud, while a fraud perpetrated against bank clients is known as a victim fraud. Collusive frauds are bank insiders conspiring with third parties, such as connected companies' fraud and deposit transformation fraud.

Fraud risk factors

When fraud is discovered, there are generally three conditions or factors present. First, and most fundamentally, opportunities must exist that allow fraud to occur — typically a deficiency in the internal control environment. Secondly, those involved in perpetrating a fraud have an identifiable incentive or believe they are under pressure to engage in fraudulent behaviour. Finally, fraudsters feel they must be able to rationalise or explain their fraudulent behaviour to themselves or others, or they must possess an attitude or set of personal principles that allow them to deviate knowingly from ethical norms.

Fraudulent financial reporting typically starts with pressure or incentive, including meeting third-party/analyst expectations, upholding debt covenants, maintaining exchange listing requirements or maintaining industry/peer performance. With respect to opportunities for fraudulent financial reporting, the most common driver is management override of controls — 'the Achilles' Heel of Fraud Prevention'.[5] Rationalisations associated with fraudulent financial reporting may include such beliefs or statements to the effect that the fraudster will 'make up for it later' or 'everybody is doing it, so why not us?'

Asset misappropriations frauds are often driven by opportunity. In other words, people will steal when the conditions that allow them to steal are present. Also, the proximate goal of most of these schemes is cash conversion. Therefore, the more cash movement there is and the more fungible and marketable an asset is, the higher the risk to the organisation. For incentives, people will often misappropriate assets to support a vice, such as gambling or drugs, or maintain a lifestyle beyond one's means (including inappropriate relationships). Rationalisations for asset misappropriation and fraudulent financial reporting differ in motivation. Fraudulent financial reporting rationalisations are frequently externalised for the perceived benefit of the organisation, while asset misappropriation rationalisations are internalised as personal. For example, we hear rationalisations for the theft of assets such as 'I am underpaid', 'the firm has treated me poorly' or 'I have worked hard, and I deserve better'. These are different from the fraudulent reporting rationalisations described earlier about the benefits to the company, firm or organisation.

It is important to note that the fraud risk factors presented above apply to both internal and external frauds — although the differences in the application may be nuanced. For instance, many internal frauds, such as fraudulent reporting schemes, are typically rationalised by the perpetrators as aiding the company. At the same time, you would not expect external fraudsters to excuse their behaviour by trying to convince someone

that they were helping the company. Indeed, much external fraud is committed by individuals or criminal syndicates whose rationalisation is similar to Willie Sutton — because the banks are where the money is.

Data analytics

Banks and financial institutions have increasingly turned to various technology solutions to assist with the detection of fraud. These technology solutions have come about rapidly. These solutions provide varying data analytic approaches from rule-based analytics, such as robotic automation, that identify red flags of typical fraudulent schemes to more advanced data analytics that deploy artificial intelligence, machine learning and behavioural analytics.

Rule-based analytics will always play a role in fraud detection. For instance, when there is not enough data available to train sophisticated models when the current state of more advanced systems does not accurately detect complex transactions or what constitutes non-compliant behaviour is discrete and well-defined. It is these types of circumstances that illustrate when rule-based approaches are appropriate. Maturing technologies, however, may offer more innovative methods for addressing emergent compliance challenges.

Emerging artificial intelligence (AI) and machine-based learning is reimagining fraud detection by moving away from solely having to depend upon past experiences to have the ability to incorporate an evaluation of emerging trends and behaviours in transaction analysis. Rather than relying entirely upon retrospective analysis, it is now possible to detect fraudulent behaviour in real time. Further, it enables bank professionals to perform fraud analytics with transaction risk scores instead of treating every possible noncompliant transaction the same, feasibly reducing time-consuming false positives.

Regardless of how advanced or mature an institution's approach is to data analytics, the core competencies of forensic professionals are indispensable in ensuring that the analytics are designed to identify, detect or predict fraud schemes accurately. In addition to a deep understanding of fraud, the forensic professional's ability to review and follow-up on anomalies identified through the analytics is essential in refining the analytics, identifying false positives and determining which outcomes require further investigation.

Next, we illustrate how the forensic perspective informs the four steps in the forensic fraud detection process. In particular, we cover the forensic techniques of detection for four serious banking-related frauds — fictitious borrowers, account takers, check kiting and rogue trading — are discussed.

THE FORENSIC FRAUD DETECTION PROCESS

The forensic fraud detection process comprises four steps: understanding (1) fraud risk factors, (2) schemes, (3) red flags and (4) detection techniques, including analytics. Each of these steps is described later and is followed by banking-related fraud schemes, which, by example, will walk us through the application of the forensic professional's perspective.

Scheme: Fictitious borrowers

Loan fraud takes many forms, including, but not limited to, fraudulent applications and valuations of collateral and fictitious borrowers. Fictitious borrowers fabricate loan documents to apply for loans that they have no intention of repaying. With some fictitious borrower schemes, commonly known as synthetic identity fraud, an individual or group develops a false identity that often blends genuine, personally identifiable information, such as Social Security numbers and addresses, to build a fabricated identity.

Sometimes, the entire identity comprises made-up details. There are numerous sites on the internet to assist fraudsters in generating false identities, including telephone numbers, addresses and zip codes, designed to pass routine bank verification. The fraudsters often build bogus identities over time to take as much money as possible. The US Department of Justice considers fictitious (synthetic identity) borrowers one of the hardest identity frauds to combat.[6]

Fictitious borrower red flags include the following:

- False identities tend to be inconsistent; as the application may contain some genuine details (eg a name that recurs in various databases), others are entirely fabricated, so they will not recur
- Cases in which the synthetic identity is entirely fictitious, the identity is too consistent, where there are no changes of mailing address, e-mail address and other identifying information
- Two or more identities associated with the same phone number
- E-mail addresses that are only a couple of months old
- The date of the oldest information is less than 12 months
- Charge-offs that occurred less than two years after opening an account
- Insignificant account activity
- No customer contact once credit limits are reached
- Frequent purchases of a single category of goods, such as high-end electronics

Methods of detection will incorporate the red flags mentioned above. With forensic input, banks and other financial institutions are moving beyond traditional methods of borrower verification by looking for unexpected patterns and relationships among applications and transactions to detect fictitious borrowers. For instance, technology can compare the entire population of account applications and match them to internet protocol (IP) addresses. Computers can even look for unexpected patterns or scan the application population to search for recurring names, Social Security Numbers (SSNs) or street addresses.

With technology, third-party data also offers practical approaches for separating genuine borrowers from fictitious borrowers. Specifically, technology can identify legitimate applicants because they have authentic backgrounds that can span years, if not decades. For instance, honest borrowers have relatively consistent street and e-mail addresses and phone numbers across various third-party databases. On the other hand, synthetic IDs are often patchy across third-party databases as they can comprise actual borrower information and fabricated information. When an ID is wholly fabricated, the ID will usually be overly consistent.

Scheme: Account takeover

Account takeovers come about when a fraudster gets unauthorised access to an account, typically changes the login credentials and personal information, and then makes fraudulent transactions with the account. These are often internal bank frauds as bank employees can misuse their access to client accounts and information. When perpetrated externally, account takeover frauds are a form of identity theft where a fraudster gets access to an account using confidential information that enables him or her to alter account settings. External fraudsters typically take advantage of data breaches, malware or phishing attacks to acquire the needed account credentials to execute unapproved transactions. Personally, identifiable information is also commonly procured illegally from dark websites. Once an account is compromised, fraudsters may steal credit card information, open lines of credit in the victim's name, wire money out of the

account and draw fraudulent checks against a compromised bank account.

Red flags for account takeover include the following:

- Changes to the online bank account profile
- Changes to the personal information associated with an account
- Disabled notifications or changes to notification details
- Changes to the online account access profile
- Changes in customer activity, such as a new IP log-on address or a login from a new device
- Access to the account at unusual times
- Small transactions processed that are quickly followed by unusually large transactions
- Significant overseas transactions

Methods of detection will seldom incorporate rule-based analytic approaches as they are relatively inadequate at uncovering account takeover schemes. Rule-based systems are designed for identifying historic schemes and cannot anticipate new methods of account compromise. Further, once a new scheme or method of compromise is detected, rules-based approaches are slow to adapt as a system professional must create new rules. AI and machine learning methods bring several advantages to combating account takeover fraud.

First, AI and machine learning methods can analyse a vast quantity of data in real time. Secondly, these methods can establish a behavioural baseline for an account holder and help compare real-time account activity to the account holder's behavioural baseline to improve suspicious activity detection. When real-time activity deviates from the established baseline, the system signals the transaction for review.

Thirdly, AI and machine learning systems can generate risk scores for each transaction. For instance, when considering the red flags above, a transaction that hits multiple fraud indicators will score higher than a transaction that hits only one red flag. Also, not all of the red flags are equally risky. For instance, an AI and machine learning system may rank overseas transactions as higher than a simple change of address. But a login from a new device to conduct an overseas transaction combined with a change of address will score even higher. As a result, false positives are reduced, and transaction follow-up is more efficient.

Scheme: Check kiting

An example of deposit account fraud described and surveyed by the ABA is check kiting. Check kiting is a frequent, external fraud scheme where nonsufficient funds (NSF) checks are deposited between two or more banks. The account balances in those banks are now inflated as the NSF checks are honoured rather than returned as unpaid. Check kiting schemes take advantage of the time lag between check deposit in one bank and presentation for payment at the bank on which drawn. Before the check clears, the fraudster writes another check on the second bank and deposits it into the first bank and afterwards merely repeats the process. When well timed, the banks will not discover that accounts are overdrawn and will continue to honour checks drawn on accounts with insufficient funds. The fraud essentially provides the schemer with an interest-free loan.

Check kiting red flags include the following:

- Numerous checks presented from nonlocal banks
- Uncommonly frequent deposits
- Check presentations from recurring financial institutions
- Unusually frequent account balance inquiries
- A short length of time on average that funds remain in an account

- Recurring issues of nonsufficient fund checks
- Erratic use of methods of deposit, for example, jumping among ATMs, after-hours deposits, drive-up tellers and multiple bank branches
- Large checks drawn in even amounts
- Recurring checks with identical signatures and payees

Check kiting AI and machine learning methods of detection analyse account holder checking activity for indicators of unusual checks. These methods may include the timing of account activity patterns in the flow of funds, the velocity of money flowing through accounts over time and the flow of funds among or between payers and payees. The systems analyse deposit and withdrawal activity and look for negative account balances. These techniques may also identify an exceptional level of deposited funds deriving from accounts under common control or through someone with multiple accounts.

Scheme: Rogue trading

A trader's job is to make trades on behalf of a bank or financial institution. Unfortunately, traders who go rouge typically work with little supervision, making unauthorised trades. While considerably less frequent than other types of fraud, perhaps the most vexing to banks is rogue trading because, as in the cases of Nick Leeson and Jerome Kerviel, the losses can be staggering. Rogue traders consciously violate financial institution trading rules, often with high-risk investments, producing massive losses or gains. Rogue trading frequently starts as an effort to make up for a lousy market position or maybe an attempt to create large commissions and bonuses. When rogue traders generate huge losses, they have typically exceeded the financial institution's trading limits and, as a result, went over the institution's loss limits. Attempts to cover up rogue trading include manipulating valuations and making unrecorded trades.

Several red flags are present when a trader has gone rogue include the following:

- Variations in a trader's transaction patterns
- The trader will not or cannot explain his or her trading strategy
- The trader does not take time off often in violation of policy
- The trader is persistently requesting higher trading limits
- The trader is unduly optimistic concerning trading strategy or positions
- The trader is persistently challenging policies, programmes or controls
- The trader's performance appears too good to be true

The velocity of the trading activity itself will easily outpace any manual review process. As such, financial institutions are turning to sophisticated machine learning technologies to review 100 per cent of trades and positions to aggregate trade data, identify unexpected or inconsistent patterns of trading activity, look for known or previously unknown types of behaviour anomalies or spot the rapid build-up of potentially dangerous positions. The technologies will also test trader system permissions, help ensure segregation of duties and review all amended and cancelled trades.

CONCLUSION

As we can understand from the previous discussion, the skills of forensic professionals have always been and will continue to be critical in helping to inform a financial institution's efforts to prevent, detect and respond to fraud. Aided by advances in data analytics, the forensic professional plays an indispensable role in providing the special expertise required to understand fraud schemes and spot the associated red flags. Forensic professionals also identify the datasets that need to

be analysed, inform the technologies applied to the analysis of the relevant data and follow up by reviewing the results of analytic procedures to eliminate false positives and detect fraud. With this knowledge, financial institutions can leverage the skills of forensic professionals to remediate control gaps and improve fraud risk management processes.

References

(1) FBI (n.d.). 'Famous cases & criminals: Willie Sutton', [Internet], available at: https://www.fbi.gov/history/famous-cases/willie-sutton (accessed 11th May, 2021).

(2) DOJ (2020). 'Justice news. Wells Fargo agrees pay $3 billion to resolve criminal and civil investigations into sales practices involving the opening of millions of accounts without customer authorization', [Internet], 21st February, available at: https://www.justice.gov/opa/pr/wells-fargo-agrees-pay-3-billion-resolve-criminal-and-civil-investigations-sales-practices (accessed 11th May, 2021).

(3) American Bankers Association (2020). 'Deposit account fraud survey', [Internet], 1st January, available at: https://www.aba.com/news-research/research-analysis/deposit-account-fraud-survey-report (accessed 11th May, 2021).

(4) Girgenti, R. H. and Hedley, T. P. (2011). *Managing the Risk of Fraud and Misconduct: Meeting the Challenges of a Global Regulated, and Digital Environment*. New York: McGraw-Hill, 1p.

(5) American Institute of Certified Public Accountants (2005). *Management Overide of Internal Controls: The Achilles' Heel of Fraud Prevention*. New York: AICPA, Title Page.

(6) Rudegeair, P. and Andriotis, A. M. (2018). 'The new ID theft: Millions of credit applicants who don't exist', WSJ, 6th March, available at: https://www.wsj.com/articles/the-new-id-theft-thousands-of-credit-applicants-who-dont-exist-1520350404 (accessed 18th June, 2021).