Discussion Paper

Fraud Detection Using Data Analytics in the Banking Industry

FREEDOM FROM DOUBT ™

ACL™

Table of Contents

What is Fraud?

Fraud encompasses a wide range of illicit practices and illegal acts involving intentional deception or misrepresentation. The Institute of Internal Auditors' International Professional Practices Framework (IPPF) defines fraud as:

"… any illegal act characterized by deceit, concealment, or violation of trust. These acts are not dependent upon the threat of violence or physical force. Frauds are perpetrated by parties and organizations to obtain money, property, or services; to avoid payment or loss of services; or to secure personal or business advantage."

Fraud impacts organizations in several areas including financial, operational, and psychological. While the monetary loss owing to fraud is significant, the full impact of fraud on an organization can be staggering. The losses to reputation, goodwill, and customer relations can be devastating. As fraud can be perpetrated by any employee within an organization or by those from the outside, it is important to have an effective fraud management program in place to safeguard your organization's assets and reputation.

Who is Responsible for Fraud Detection?

While senior management and the board are ultimately responsible for a fraud management program, internal audit can be a key player in helping address fraud. By providing an evaluation on the potential for the occurrence of fraud, internal audit can show an organization how it is prepared for and is managing these fraud risks.

In today's automated world, many business processes depend on the use of technology. This allows for people committing fraud to exploit weaknesses in security, controls or oversight in business applications to perpetrate their crimes. However, the good news is that technology can also be a means of combating fraud. Internal audit needs to view technology as a necessary part of their toolkit that can help prevent and detect fraud. Leveraging technology to implement continuous fraud prevention programs helps safeguard organizations from the risk of fraud and reduce the time it takes to uncover fraudulent activity. This helps both catch it faster and reduce the impact it can have on organizations.

The International Professional Practices Framework (IPPF) contains the following Standards on fraud and internal audit's role:

1200 – Proficiency and Due Professional Care

1210-A2 – Internal auditors must have sufficient knowledge to evaluate the risk of fraud and the manner in which it is managed by the organization, but are not expected to have the expertise of a person whose primary responsibility is detecting and investigating fraud.

1220 – Due Professional Care

1220.A1 – Internal auditors must exercise due professional care by considering the following:

- Extent of work needed to achieve the engagement's objectives;
- Related complexity, materiality, or significance of matters to which assurance procedures are applied;
- Adequacy and effectiveness of governance, risk management, and control processes;
- Probability of significant errors, fraud, or noncompliance; and
- Cost of assurance in relation to potential benefits.

2060 – Reporting to Senior Management and the Board

The chief audit executive must report periodically to senior management and the board on the internal audit activity's purpose, authority, responsibility, and performance relative to its plan. Reporting must also include significant risk exposures and control issues, including fraud risks, governance issues, and other matters needed or requested by senior management and the board.

2120 – Risk Management

2120.A2 – The internal audit activity must evaluate the potential for the occurrence of fraud and how the organization manages fraud risks.

2210 – Engagement Objectives

2210.A2 – Internal auditors must consider the probability of significant errors, fraud, noncompliance, and other exposures when developing the engagement objectives.

Why Use Data Analysis for Fraud Detection?

Data analysis technology enables auditors and fraud examiners to analyze an organization's business data to gain insight into how well internal controls are operating and to identify transactions that indicate fraudulent activity or the heightened risk of fraud. Data analysis can be applied to just about anywhere in an organization where electronic transactions are recorded and stored.

Data analysis also provides an effective way to be more proactive in the fight against fraud. Whistleblower hotlines provide the means for people to report suspected fraudulent behavior but hotlines alone are not enough. Why be only reactive and wait for a whistleblower to finally come forward? Why not seek out indicators of fraud in the data? That way, organizations can detect indicators of fraudulent activity much sooner and stop it before it becomes material and creates financial damage.

The Association of Certified Fraud Examiners' 2010 Global Fraud Study *found that the* ***banking and financial services industry*** *had the most cases across all industries – accounting for more than 16% of frauds.*

www.acfe.org

To effectively test for fraud, all relevant transactions must be tested across all applicable business systems and applications. Analyzing business transactions at the source level helps auditors provide better insight and a more complete view as to the likelihood of fraud occurring. It helps focus investigative action to those transactions that are suspicious or illustrate control weaknesses that could be exploited by fraudsters. Follow-on tests should be performed to further that auditor's understanding of the data and to search for symptoms of fraud in the data.[1]

There is a spectrum of analysis that can be deployed to detect fraud. It ranges from point-in-time analysis conducted in an ad hoc context for one-off fraud investigation or exploration, through to repetitive analysis of business processes where fraudulent activity is likely to more likely to occur. Ultimately, where the risk of fraud is high and the likelihood is as well, organizations can employ an "always on" or continuous approach to fraud detection – especially in those areas where preventative controls are not possible or effective.

Once an organization gets started with data analysis, they usually find that they want to do more and dig deeper into the data. Modern organizations have increased management demands for information and the audit paradigm is shifting from the traditional cyclical approach to a continuous and risk-based model. Technology therefore offers a range of solutions, varying by the size and sophistication of the audit organization. From ad hoc analysis, through to repeatable automated procedures, and continuous auditing and monitoring, analytics provide insight into the integrity of financial and business operations through transactional analysis. Technology provides more accurate audit reports and better insight into the internal controls framework, and improves the ability to access and manage business risk.

[1] Coderre, David G., *Fraud Analysis Techniques Using ACL*, John Wiley & Sons, 2009.

Analytical Techniques for Fraud Detection

Getting started requires an understanding of:

- ✓ The areas in which fraud can occur
- ✓ What fraudulent activity would look like in the data
- ✓ What data sources are required to test for indicators of fraud

The following techniques are effective in detecting fraud. Auditors should ensure they use these, where appropriate. They include the following:

- **Calculation of statistical parameters** (e.g., averages, standard deviations, high/low values) – to identify outliers that could indicate fraud.
- **Classification** – to find patterns amongst data elements.
- **Stratification of numbers** – to identify unusual (i.e., excessively high or low) entries.
- **Digital analysis using Benford's Law** – to identify unexpected occurrences of digits in naturally occurring data sets.
- **Joining different diverse sources** – to identify matching values (such as names, addresses, and account numbers) where they shouldn't exist.
- **Duplicate testing** – to identify duplicate transactions such as payments, claims, or expense report items.
- **Gap testing** – to identify missing values in sequential data where there should be none.
- **Summing of numeric values** – to identify control totals that may have been falsified.
- **Validating entry dates** – to identify suspicious or inappropriate times for postings or data entry.[2]

> *"As a large multinational organisation, our internal audit process is under scrutiny from multiple global and local authorities. It was essential for us to find a solution which allowed fast processing of financial data, was scalable to our needs and streamlined the entire process to increase overall efficiency. ACL met every one of our needs."*
>
> **Cyrille Oudard**
> *Head of Internal Audit Tools, BNP Paribas*

Please note that random sampling is not listed as an effective fraud detection technique. While sampling is an effective data analysis technique for analyzing data values that are consistent throughout the data population, the very nature of fraud is different as it tends not to occur randomly.

[2] *Global Technology Audit Guide: Fraud Prevention and Detection in an Automated World*. The Institute of Internal Auditors, 2009.

Fraud Detection Program Strategies

Instead of relying on reactive measures like whistleblowers, organizations can and should take a more hands-on approach to fraud detection. A fraud detection and prevention program should include a range of approaches – from point-in-time to recurring and, ultimately, continually for those areas where the risk of fraud warrants. Based on key risk indicators, point-in-time (or ad hoc) testing will help identify transactions to be investigated. If that testing reveals indicators of fraud, recurring testing or continuous analysis should be considered.

A KPMG Forensics' Fraud Risk Management report states, "unlike retrospective analyses, continuous transaction monitoring allows an organization to identify potentially fraudulent transactions on, for example, a daily, weekly, or monthly basis. Organizations frequently use continuous monitoring efforts to focus on narrow bands of transactions or areas that pose particularly strong risks."[3]

By leveraging the power of data analysis technology organizations can detect fraud sooner and reduce the negative impact of significant losses owing to fraud.

> *"ACL AuditExchange leverages ACL's proven analytical strengths and Informatica's data integration capabilities to provide auditors with a means to perform data analyses and help effectively detect and prevent fraud."*
>
> **David Coderre**
> leading author of books such as "Computer-Aided Fraud Detection & Prevention: A Step-by-Step Guide"

[3] "Fraud Risk Management: Developing a Strategy for Prevention, Detection and Response." KPMG International, 2006

Banking

Fraud detection in banking is a critical activity that can span a series of fraud schemes and fraudulent activity from bank employees and customers alike. Since banking is a relatively highly regulated industry, there are also a number of external compliance requirements that banks must adhere to in the combat against fraudulent and criminal activity.

Banking/Financial Services – 298 Cases		
Scheme	Number of Cases	Percent of Cases
Corruption	101	33.9%
Cash on Hand	64	21.5%
Billing	37	12.4%
Check Tampering	35	11.7%
Non-Cash	33	11.1%
Skimming	32	10.7%
Larceny	29	9.7%
Expense Reimbursements	20	6.7%
Financial Statement Fraud	16	5.4%
Payroll	9	3.0%
Register Disbursements	8	2.7%

Distribution of Fraud Schemes in Banking/Financial Services [4]

Banking Related Fraud Schemes:

Here are a few typical fraud schemes encountered in banking and some examples of the way data analysis can be applied to detect and prevent them:

Corruption

- Find customers who appear on the US Treasury Department Office of Foreign Asset Control (OFAC) list.
- Ensure Financial Action Taskforce on Money Laundering (FATF) compliance.
- Produce listing of transactions with organizations on the list of non-cooperative countries and territories.

Cash

- Identify cash transactions just below regulatory reporting thresholds.
- Identify a series of cash disbursements by customer number that together exceed regulatory reporting thresholds.
- Identify statistically unusual numbers of cash transfers by customer or by bank account.

Billing

- Identify unusually large number of waived fees by branch or by employee.

Check Tampering

- Identify missing, duplicate, void or out of sequence check numbers.
- Identify checks paid that do not match checks issued, by bank, by check.
- Locate check forgery or falsification of loan applications.

[4] *2010 Global Fraud Study: Report to the Nations on Occupational Fraud and Abuse*, Association of Certified Fraud Examiners

Skimming

- Highlight very short time deposit and withdrawal on the same account.
- Find indicators of kiting checks.
- Highlight duplication of credit card transactions and skimming.

Larceny

- Identify customer account takeover.
- Identify co-opted customer account information.
- Locate number of loans by customer or bank employee without repayments.
- Find loan amounts greater than the value of specified item or collateral.
- Highlight sudden activity in dormant customer accounts – identify who is processing transactions against these accounts.
- Isolate mortgage fraud schemes – identify “straw buyer” scheme indicators.

Financial Statement Fraud

- Monitor dormant and suspense General Ledger accounts.
- Identify Journal Entries at suspicious times.

Other Resources

- **Association of Certified Fraud Examiners (ACFE):** the world's largest anti-fraud organization and premier provider of anti-fraud training and education. **www.acfe.org**
- **The Institute of Internal Auditors (The IIA)**: **www.theiia.org**
  - » *International Standards for the Professional Practice of Internal Auditing (Standards):* The *Standards* are mandatory requirements – principle-focused and providing a framework for performing and promoting internal auditing.
  - » *Internal Auditing and Fraud Practice Guide:* guidance on how to comply with the International Standards for the Professional Practice of Internal Auditing.
  - » *GTAG 13: Fraud Prevention and Detection Techniques in an Automated World*: step-by-step process guide for auditing a fraud prevention program, including an explanation of the various types of data analysis to use in detecting fraud, and a technology fraud risk assessment template.
- **ACL Detecting Fraud resource page**: anti-fraud materials including industry reports, case studies and on-demand webinars. **www.acl.com/bankingfraud**

To find out how ACL can help your organization combat fraud, contact us at ***+1-604-669-4225*** *or* ***info@acl.com*** *to arrange for a free consultation.*

About ACL Services Ltd.

ACL Services Ltd. is the leading global provider of business assurance technology for audit and compliance professionals. Combining market-leading audit analytics software with centralized content management and exception reporting, ACL technology provides a complete end-to-end business assurance platform that is flexible and scalable to meet the needs of any organization.

Since 1987, ACL technology has helped organizations reduce risk, detect fraud, enhance profitability and improve business performance. ACL delivers its solutions to 14,000 organizations in over 150 countries through a global network of ACL offices and channel partners. Our customers include 95 percent of Fortune 100 companies, 85 percent of the Fortune 500 and over two-thirds of the Global 500, as well as hundreds of national, state and local governments, and the Big Four public accounting firms. www.acl.com

DP/BNK/200710