

# Fraud and Data Mining

---

Deposit Account Fraud

# Contents

---

- What is Fraud
- Common types of Fraud
- How to detect Fraud
- How to prevent Fraud
- Questions

# What is fraud

---

- An act of deception carried out for the purpose of unfair, undeserved, and/or unlawful gain, especially financial gain.
- While there are many types of fraud, some of which most financial institutions may encounter are:
  - Bankruptcy Fraud
  - Bribery
  - Computer Fraud
  - Credit Card Fraud
  - Counterfeiting
  - Embezzlement
  - Extortion
  - Forgery
  - Identity theft
  - Money Laundering



# What is fraud (Cont.)

---

There are two fraud Categories

- First Party Fraud – a fraud committed by an individual on their own account, for their own benefit. In all instances of first party fraud, the client is the fraudster.

*Client knowingly deposits a worthless cheque or an empty envelope in an ABM*

- Third Party Fraud – a fraud committed by an individual other than the victim, for the purpose of financial gain at someone else's expense.

- Third Party – First party fraud

*Fraudster skims victim's card information and uses that to withdraw funds from an account*

- Third party – Friendly fraud

*Roommate takes client's debit card and withdraws funds from the client's account without the client's knowledge or consent*

- Third party – Recruitment fraud

*Client cashes a cheque for another individual, and the individual for whom the cheque was cashed knows that the cheque is forged*

# Common types of Fraud

---

- Account Takeover (3<sup>rd</sup> party)

A fraud committed when an individual pretends to be an existing client and takes control of the legitimate client's account for the purposes of removing the funds from the account or using the account to deposit fraudulent items.

- Bust Out (1<sup>st</sup> party)

A fraud committed when a client who has been a good customer for a period of time, uses this behavior to gain large access to funds, which they then use, with no intention of repayment. (Frequently committed when a person is leaving the country and a negative bureau will not impact them)

- Counterfeit (1<sup>st</sup> or 3<sup>rd</sup> party)

A fraud committed when an individual creates a phoney item and passes it off as legitimate.

- Defalcation(1<sup>st</sup> party)

A fraud committed when an employee uses their position within the company to commit any type of fraud.

# Common types of Fraud (Cont.)

---

- Kiting (1<sup>st</sup> party)

A fraud committed when a client deliberately moves funds between two or more accounts at same/different branches or Financial Institutions to disguise a lack of funds.

- Phishing (a.k.a. spoofing, 3<sup>rd</sup> party)

A fraud committed when an individual uses fraudulent e-mail and web pages to gather personal, financial and sensitive information from various individuals, for the purposes of identity theft.

- Skimming (3<sup>rd</sup> party)

A fraud committed when the information contained within the magnetic strip on the back of an individual's card has been obtained without consent and then used to re-emboss and/or re-encode fraudulent cards with real data. For debit card skims, the PIN is also captured along with the mag stripe data.

# Common types of Fraud (Cont.)

---

- True Name Fraud (3<sup>rd</sup> party)

A fraud committed when another individual's identity is assumed for the purpose of establishing and obtaining accounts and credit against that individual's name and credit history.

- True SIN Fraud (3<sup>rd</sup> party)

A fraud committed when another individual's SIN is obtained and a false identity is created for the purpose of establishing and obtaining accounts and credit against that individual's SIN and credit history.

- Worthless Deposit (1<sup>st</sup> party)

A fraud committed when a client deposits an item(s) that will not be cleared (e.g. NSF item, counterfeit cheque), for the purpose of withdrawing money against the access to funds on the account.

# How to Detect Fraud

## Worthless deposits

---

- There are several ways in which transactions are analyzed in order to determine if they are fraud, two of which are:
  - Near real time monitoring – Risky transactions are flagged based on a set of rules determined through analysis of transaction history.  
Based on risk flag the transaction is forwarded to a consultant who immediately takes further action in determining the possibility of fraud.  
The risk rules that are in effect during the live monitoring are constantly updated and tested through data mining.
  - Delayed Risk model – Transactions are ranked based on risk levels determined by transaction risk model.  
These transactions are then reviewed with a one day delay in order to determine the possibility of fraud.  
There are risk model performance tracking procedures in place that monitor the effectiveness of these risk models in order to detect deterioration of the risk model and prompt for updating of the model.

# How to Prevent Fraud

## Skimming

---

- Skimming fraud can be prevented at two different points.
  - In order for the fraudster to obtain magnetic strip information and PIN numbers from individuals using a specific ABM, they need to tamper with the ABM and place a mag. Strip reader as well as a camera to obtain PIN number information.

One way to stop the tamper from happening is to alter the ABM machine in such a way to prevent the fraudster from placing a mag. Strip reader or placing a camera to capture the PIN number.
  - Once a fraudster has obtained the card information required, they will need to create card copies and withdraw funds.

The fraudster can be stopped at this point with the help of near real time monitoring systems that flag risky behavior at ABM machines.