Stephen Dornu Dugbartey
Edmonton, Alberta – Canada | +1 (825) 777-0501 | ddstephen07@gmail.com

Electronic Banking Fraud Risk Analysis

1.0 Executive Summary

Background

Banks cannot survive competition and utmost value creation without relying on electronic banking services such as mobile applications, internet banking, debit/credit cards. The services have increased convenience for customers, but have also created vulnerabilities and cyber threats which can cause a weak basis for fraud to occur.

Project Objective:

The objective of this project is prioritizing, a standard-guided view of electronic banking fraud risks that will enable management to proactively strengthen controls while optimizing fraud detection efficiency. The objective is broken into three (3) activities:

- Identify and analyse risk areas of using electronic banking services with sample datasets generated
- Assess the likelihood and impact of each risk area to inform priority and resource allocation
- Recommend fraud risk prevention, detection, and correction techniques guided by the NIST SP-800 53r5

Project Scope:

- 100 transactions of electronic banking nature were selected
- 50 customers were involved with the selected datasets
- 4 account types were involved: checking, savings, credit card and debit card
- 4 channels were deployed for customers: POS, ATM, mobile app and internet banking
- The transactions were performed between January 2025 and September 2025
- 6 merchant categories were the focus: food, service, electronic, entertainment, travel and retail
- 4 authentication types were the focus: biometric, OTP, password and PIN

Tools Deployed:

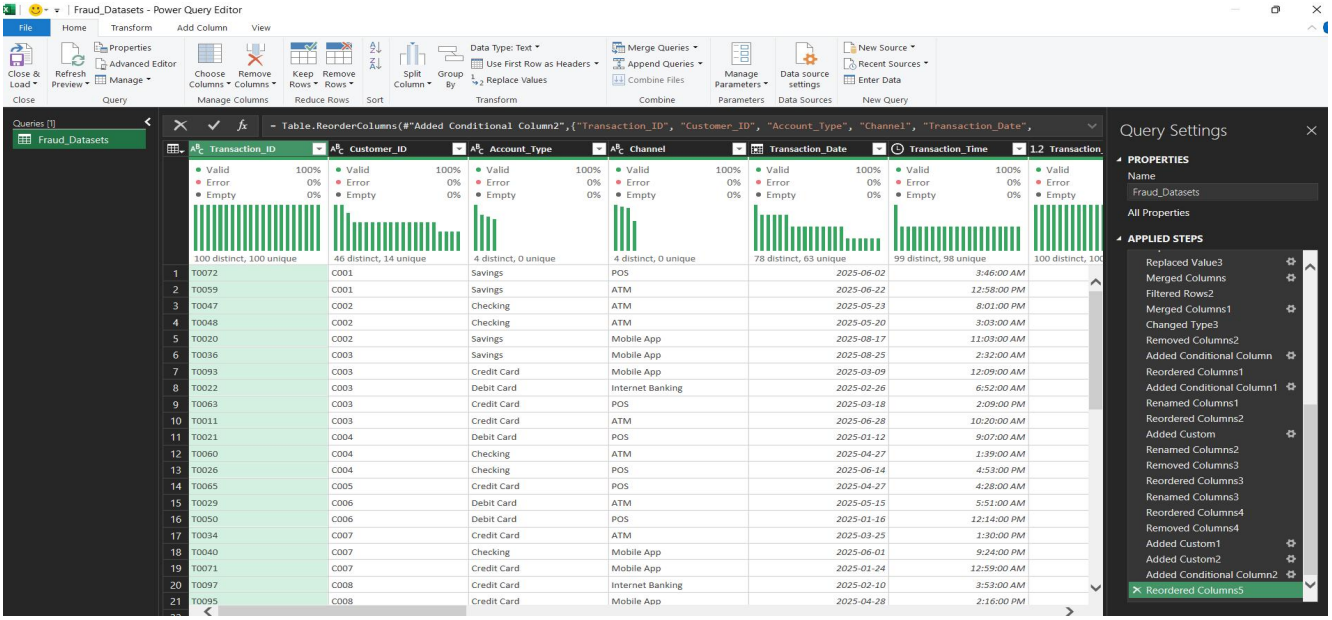
- Microsoft Excel
- Power Query
- Pivot Tables
- Excel charts
- Semi-quantitative risk metrics
- NIST SP 800-53r5

2.0 Methodology

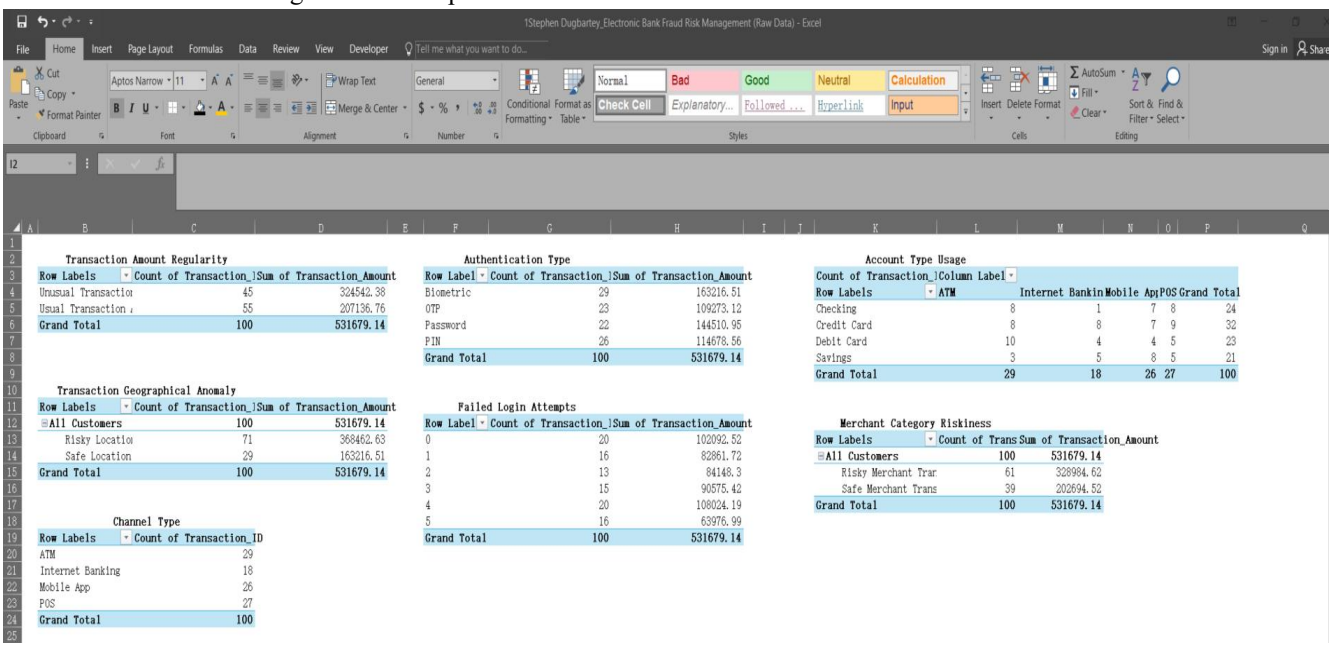
The following method was deployed:

- Acquired sample datasets relating to fraud transactions in the use of electronic banking services. 100 transactions were generated to include the columns: ***Transaction ID, Customer ID, Account type, Channel of transactions, Transaction date, Transaction amount, Device ID, Merchant category, Authentication type, Login failure counts, Country of residence, and Country of transaction.***

- The datasets were cleaned with Microsoft Power Query. Some columns were conditionally created to define the nature of risk analyzed.
  For example: the average transaction amount of each customer was calculated and compared to the transaction value of the same customer to determine unusual transactions of each customer.
  Where the transaction value is greater than the average transaction amount of the same customer, possible risk may exist for investigation.



- Pivot tables were generated into possible fraud risk areas for focus and further assessment



Transaction Amount Regularity

Row Labels	Count of Transaction_ID	Sum of Transaction_Amount
Unusual Transactio	45	324542.38
Usual Transaction	55	207136.76
Grand Total	100	531679.14

Authentication Type

Row Label	Count of Transaction_ID	Sum of Transaction_Amount
Biometric	29	163216.51
OTP	23	109273.12
Password	22	144510.95
PIN	26	114678.56
Grand Total	100	531679.14

Account Type Usage

Count of Transaction_ID	Column Label				
Row Labels	ATM	Internet Bankin	Mobile App	POS	Grand Total
Checking	8	1	7	8	24
Credit Card	8	8	7	9	32
Debit Card	10	4	4	5	23
Savings	3	5	8	5	21
Grand Total	29	18	26	27	100

Transaction Geographical Anomaly

Row Labels	Count of Transaction_ID	Sum of Transaction_Amount
All Customers	100	531679.14
Risky Location	71	368462.63
Safe Location	29	163216.51
Grand Total	100	531679.14

Failed Login Attempts

Row Label	Count of Transaction_ID	Sum of Transaction_Amount
0	20	102092.52
1	16	82861.72
2	13	84148.3
3	15	90575.42
4	20	108024.19
5	16	63976.99
Grand Total	100	531679.14

Merchant Category Riskiness

Row Labels	Count of Trans	Sum of Transaction_Amount
All Customers	100	531679.14
Risky Merchant Trar	61	328984.62
Safe Merchant Trans	39	202694.52
Grand Total	100	531679.14

Channel Type

Row Labels	Count of Transaction_ID
ATM	29
Internet Banking	18
Mobile App	26
POS	27
Grand Total	100

- Risk metrics (the likelihood and impact) was defined
- The risk was used to assess the risk areas to ascertain their existence and impact
- Microsoft Excel was used to create a dashboard summary of the findings
- Strategies were recommended to prevent, detect, and correct identified risk areas based on NIST SP 800-53r5

Data Limitations

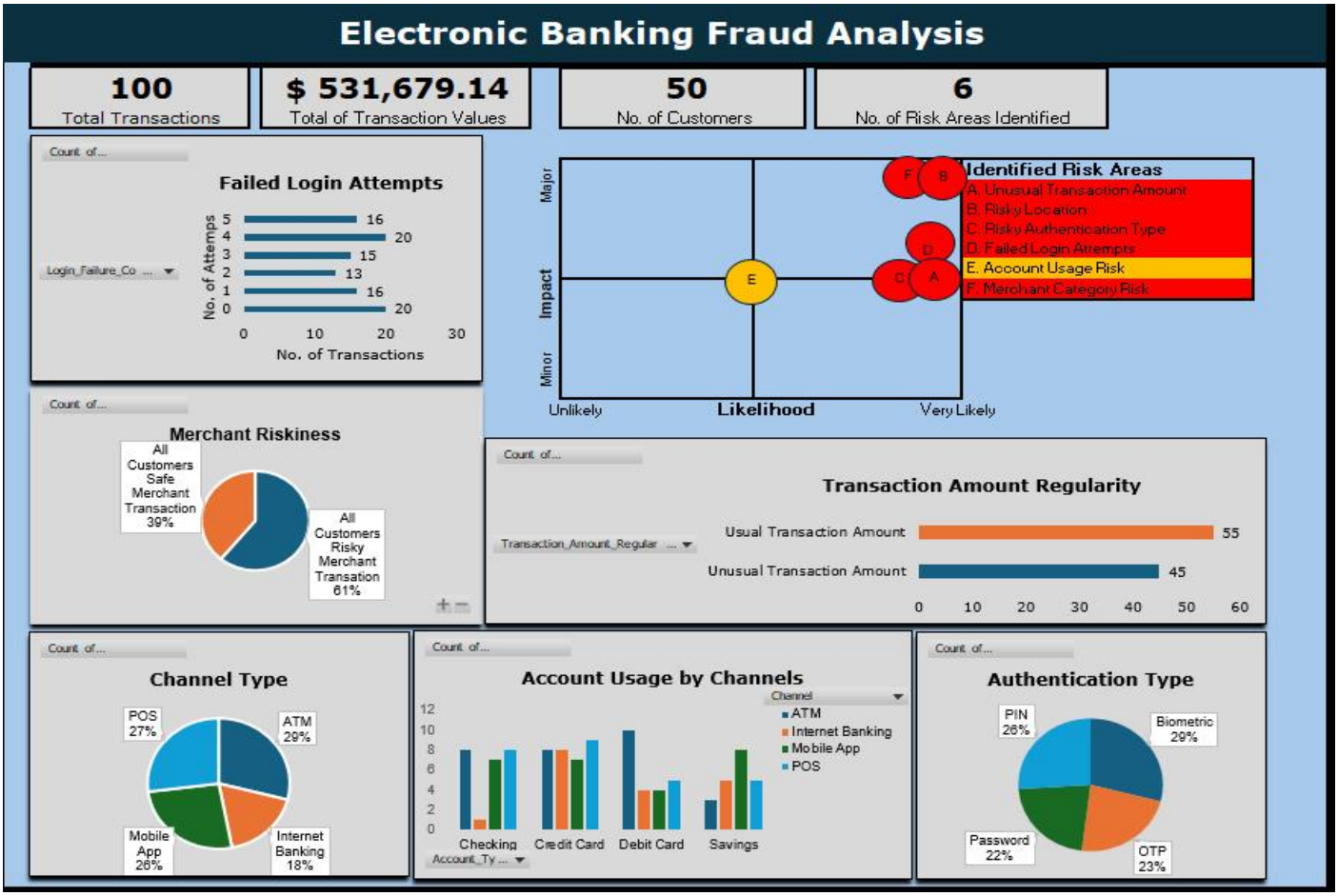
- Some fraud events may not be captured or incorrectly labeled in transaction logs.Some missing fields may include device ID, geographical location, and channels
- Fraudsters continuously change tactics to evade detection rules. Historical datasets may not reflect current or emerging fraud patterns.
- Strict privacy laws and internal policies limit access to sensitive data. Analysts may work with authorized data datasets only.

3.0 Project Findings

After analysing the generated datasets, six (6) fraud risk areas were identified as follows:

- Unusual transaction amount.
- Risky transaction by geography.
- Risky transaction by authentication type
- Risk of failed login attempts
- Inappropriate account type usage
- Risky transaction by merchant category

A summary of the outcome is shown in the dashboard below:



Root Causes of Vulnerabilities with Electronic Banking:

- ***Weak authentication and access controls***. The electronic products of the bank work on different platforms connected over the internet. A weak password policy, weak multi-factor authentication and inadequate session management can cause some of these fraud risks to occur.
- ***Inadequate transaction monitoring and fraud detection***. Fraud events are dynamic with time, hence static rules and poor alert escalation will not help the bank adapt to and detect new fraud patterns.
- ***Vulnerabilities in applications and infrastructure security***. Architectural weaknesses in applications and IT infrastructure security can occur with outdated software, unpatched systems, weak encryption implementation and insecure API connecting banking systems.
- ***Non-compliance with security standards*.** The bank may have improper network segregation, or weak logging and monitoring of card transactions as recommended by NIST SP-800r5, or inadequate protection of cardholder data as recommended by PCI-DSS.
- ***Limited user awareness and social engineering controls.*** The bank may not have created enough awareness for their customers about social engineering and security practices required to stay safe while using the bank's electronic platforms. The staff of the bank may also not have adequate training or education regarding security and privacy trends to protecting customers.

Risk Impact to the Bank

Related fraud with the use of electronic banking products could result in the following risks:

- ***Financial loss to the customers and bank***. Unauthorized withdrawals could cause loss of customers while reimbursement and charge back will cost the bank's in the fraud event.
- ***Regulatory and compliance risk***. The fraud event could trigger regulatory findings for breach with consumer protection laws which may result in fines or stricter supervision conditions.
- ***Customer experience and reputation risk***. Customers may lose trust in the bank with their fraud experiences particularly, if the same fraud trend continues
- ***Operational disruption***. To resolve fraud occurrences, emergency shutdowns and high volumes of customer complaints will increase workload for fraud and customer support teams taking up existing financial resources, IT resources, human resources and time.
- ***Control breakdown and inefficiencies***. The need to correct errors will result in increased human intervention which may result in more errors and dire impacts.
- ***Legal and liability risk***. Customers may embark on lawsuits. Unbearable numbers of such lawsuits could shut down the bank's operations.

4.0 Details of Risk Areas Identified

Unusual Transaction Amount

The average transaction of each customer is compared to individual transactions performed by that same customer. Risk is identified where the actual transaction is greater than the average transaction amount for the same customer. It shows an unusual pattern traceable to the customer. 45 transactions were identified as unusual. The total value exposed with this risk is $324,542.38.

Transaction Amount Regularity

Row Labels	Count of Transaction_ID	Sum of Transaction_Amount
Unusual Transaction Amount	45	324542.38
Usual Transaction Amount	55	207136.76
Grand Total	**100**	**531679.14**

Risky Authentication Type

Biometric and OTP are more secure authentication than password or PIN because they involved a direct involment of the actual customer to validate. 48 transactions are identified at risk with the use of password or PIN only. $259,189.51 is value is at risk.

Authentication Type

Row Labels	Count of Transaction_ID	Sum of Transaction_Amount
Biometric	29	163216.51
OTP	23	109273.12
Password	22	144510.95
PIN	26	114678.56
Grand Total	**100**	**531679.14**

Failed Login Attempts

51 transactions with 3 or more failed login attempts are a risk because the actual customer is likely to recall their login credentials by the second attempt. $262,576.60 worth of transactions is at risk

Failed Login Attempts

Row Labels	Count of Transaction_ID	Sum of Transaction_Amount
0	20	102092.52
1	16	82861.72
2	13	84148.3
3	15	90575.42
4	20	108024.19
5	16	63976.99
Grand Total	**100**	**531679.14**

Risky Location Transaction

Where the country of residence differs from the country of transaction and the authentication type is neither biometric nor OTP, the geographical location is risky with the transaction performed. Biometric and OTP give reasonable assurance that the customer is performing the transactions themselves away from where the bank knows them on record to reside. 71 transactions were identified as risky locations with $368,462.63 exposed.

Transaction Geographical Anomaly

Row Labels	Count of Transaction_ID	Sum of Transaction_Amount
All Customers	**100**	**531679.14**
Risky Location	71	368462.63
Safe Location	29	163216.51
Grand Total	**100**	**531679.14**

Account Type Usage Risk

Checking accounts, credit cards and debit cards are usually transactional in nature but an ATM or POS usage on savings accounts exposes risk with the inappropriate account usage which defeats the savings purpose of that account. 8 transactions and $30,813.08 have been identified to be at risk based on account type usage.

Account Type Usage

Count of Transaction_ID Row Labels	ATM	Internet Banking	Mobile App	POS	Grand Total
Checking	8	1	7	8	24
Credit Card	8	8	7	9	32
Debit Card	10	4	4	5	23
Savings	3	5	8	5	21
Grand Total	**29**	**18**	**26**	**27**	**100**

Merchant Category Riskiness

If the country of residence differs from the country of transaction and the merchant category is either electronics or travel, risk is higher. A customer will highly plan purchases of an electronic or travel nature and will usually perform such transactions from their country of residence. When electronic or travel expenses are paid from outside the country of residence, there is some level of risk that it may not be the actual customer of the bank performing that transaction. $328,984.62 and 61 transactions are at risk based on merchant category.

Merchant Category Riskiness

Row Labels	Count of Transaction_ID	Sum of Transaction_Amount
All Customers	**100**	**531679.14**
Risky Merchant Transation	61	328984.62
Safe Merchant Transaction	39	202694.52
Grand Total	**100**	**531679.14**

5.0 Risk Metrics

The risk metrics is defined by the risk level rating, likelihood rating and impact rating.

Risk Level

Risk level rating is defined by the **likelihood rating** and **impact rating** of each risk area.

Risk Level	Rating
Low Risk	2 and below
Medium Risk	3 - 4
High Risk	5 and above

Likelihood

Defined as the possibility of the risk area occurring. The number of the affected transaction expressed as a percentage of the total number of transactions observed defines the possibility.

Likelihood	Percentage Referred	Rating
Unlikely	Less than 5%	1
Likely	Between 6% and 40%	2
Very Likely	Higher than 40%	3

Impact

Defined as the amount value that can be affected in relation to the expressed likelihood.

Impact Severity	Amount Impacted	Rating	Investigation and Resolution Timeline
Minor	Less than $100,000	1	Up to 2 months
Serious	Between $100,001 and $300,000	2	Up to 1 month
Major	Higher than $300,000	3	Up to 1 week

Fraud Risk Area Risk Assessment Summary

Risk Category	Likelihood		Impact Severity		Risk Rating	Risk Level
	Percentage	Rating	Amount	Rating		
Unusual Transaction Amount	45%	3	$324,542.38	3	5	High
Risky Location	71%	3	$368,462.63	3	6	High
Risky Authentication Type	48%	3	$259,189.51	2	5	High
Failed Login Attempts	51%	3	$262,576.6	2	5	High
Account Usage Risk	8%	2	$30,813.08	1	3	Medium
Merchant Category Risk	61%	3	$328,984.62	3	6	High

6.0 Risk Areas and Required Strategies

Due to scarce resources and budget constraints, the assessed risk areas must be prioritized considering the overall risk rating and the impact severity amounts. Controls to assist prevent, detect and correct the identified risk areas using the NIST SP 800-53r5 have been recommended.

Risk Category	Recommended Controls based on NIST SP 800-53r5	Implementation Timelines	Responsibility
1. Risky Locations Transactions 2. Risky Merchant Category Transaction 3. Failed login Attempts Risk 4. Risky Authentication Type 5. Unusual Transaction Amount 6. Account Usage Risk	AC-18: Wireless Access AC-19: Access Control for Mobile Devices AU-6: Audit Record Review, Analysis and Reporting AU-8: Time Stamps CA-3: Information Exchange CA-7: Continuous Monitoring CP-9: System Backup IA-3: Device Identification and Authentication IA-8: User Identification and Authentication RA-5: Vulnerability Monitoring and Scanning	Within 1 month And Up to a week regular review and reporting	**IT and IS Steering Committee** ● Chief Risk Officer ● Chief Information Officer ● Chief Financial Officer ● Chief Compliance Officer ● Head, Legal ● Head of Internal Audit ● Head, Human Resources ● Various Departmental Heads
	RA-7: Risk Response	Within 1 week And Monthly review and reporting	
	AT-2: Literacy Training and Awareness CA-2: Control Assessments SC-12: Cryptographic Key Establishment and Management	Within 1 month And Monthly review and reporting	
	CM-4: Impact Analyses RA-3: Risk Assessment	Within the next quarter And Quarterly review and reporting	
	CP-2: Contingency Plan IR-8: Incident Response Plan	Within the next quarter And Annual review and reporting	