Stephen Dornu Dugbartey

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

Project: Risk Management
Fraud Detection and Analysis with Using Electronic Banking Services by Customers

1.0 Project Background

The growth of electronic banking services such as mobile applications, internet banking, debit/credit cards has increased convenience for customers, but it has also created opportunities for bad actors and cyber threats. Cybercriminals, insiders, third-party providers, and customers exploit weaknesses in banking systems for fraud to occur.

Project Objective:

The objective of this project analyzes various risks capable of causing fraud associated with the use of electronic banking products by customers. The objective is broken into four (4) areas:

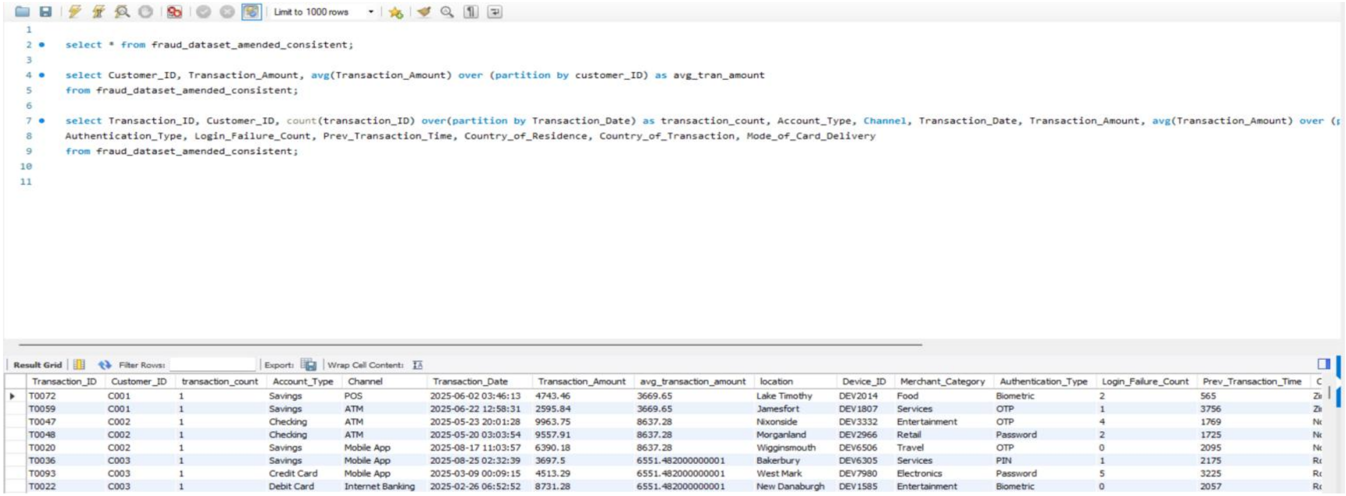
- Identify and analyse risk areas of using electronic banking services with sample datasets generated
- The risk matrix applied to each risk area is assessed to determine its likelihood and impact to inform priority and resource allocation
- Recommend risk prevention, detection, and correction techniques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

Methodology:

The following methods were deployed:

- Acquired sample datasets relating to fraud transactions in the use of electronic banking services. 100 transactions were generated to include: ***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.***

- SQL was used to customise the generated datasets. For example, the average transaction amount partitioned by customer ID was added.



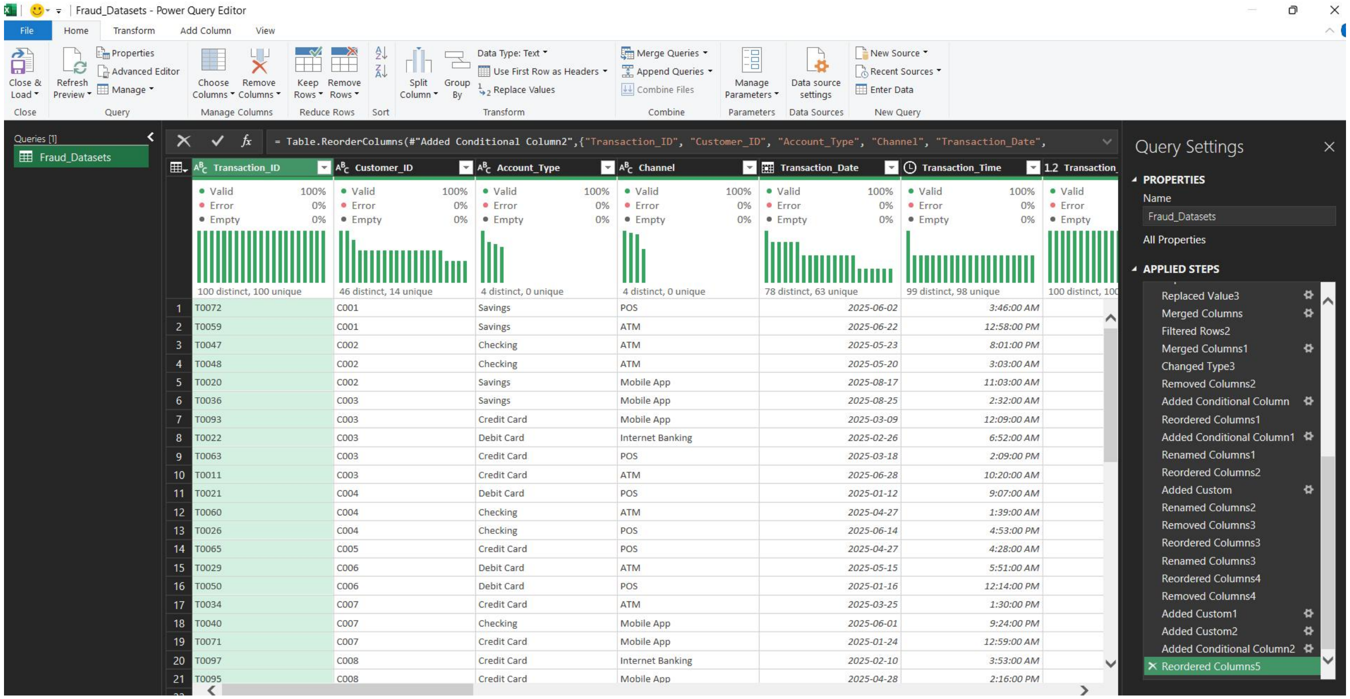
```sql
select * from fraud_dataset_amended_consistent;

select Customer_ID, Transaction_Amount, avg(Transaction_Amount) over (partition by customer_ID) as avg_tran_amount
from fraud_dataset_amended_consistent;

select Transaction_ID, Customer_ID, count(transaction_ID) over(partition by Transaction_Date) as transaction_count, Account_Type, Channel, Transaction_Date, Transaction_Amount, avg(Transaction_Amount) over (p
Authentication_Type, Login_Failure_Count, Prev_Transaction_Time, Country_of_Residence, Country_of_Transaction, Mode_of_Card_Delivery
from fraud_dataset_amended_consistent;
```

Transaction_ID	Customer_ID	transaction_count	Account_Type	Channel	Transaction_Date	Transaction_Amount	avg_transaction_amount	location	Device_ID	Merchant_Category	Authentication_Type	Login_Failure_Count	Prev_Transaction_Time	C
T0072	C001	1	Savings	POS	2025-06-02 03:46:13	4743.46	3669.65	Lake Timothy	DEV2014	Food	Biometric	2	565	Zi
T0059	C001	1	Savings	ATM	2025-06-22 12:58:31	2595.84	3669.65	Jamesfort	DEV1807	Services	OTP	1	3756	Zi
T0047	C002	1	Checking	ATM	2025-05-23 20:01:28	9963.75	8637.28	Nixonside	DEV3332	Entertainment	OTP	4	1769	Nc
T0048	C002	1	Checking	ATM	2025-05-20 03:03:54	9557.91	8637.28	Morganland	DEV2966	Retail	Password	2	1725	Nc
T0020	C002	1	Savings	Mobile App	2025-08-17 11:03:57	6390.18	8637.28	Wigginsmouth	DEV6506	Travel	OTP	0	2095	Nc
T0036	C003	1	Savings	Mobile App	2025-08-25 02:32:39	3697.5	6551.482000000001	Bakerbury	DEV6305	Services	PIN	1	2175	Rc
T0093	C003	1	Credit Card	Mobile App	2025-03-09 00:09:15	4513.29	6551.482000000001	West Mark	DEV7980	Electronics	Password	5	3225	Rc
T0022	C003	1	Debit Card	Internet Banking	2025-02-26 06:52:52	8731.28	6551.482000000001	New Danaburgh	DEV1585	Entertainment	Biometric	0	2057	Rc

- The datasets were cleaned with Microsoft Power Query



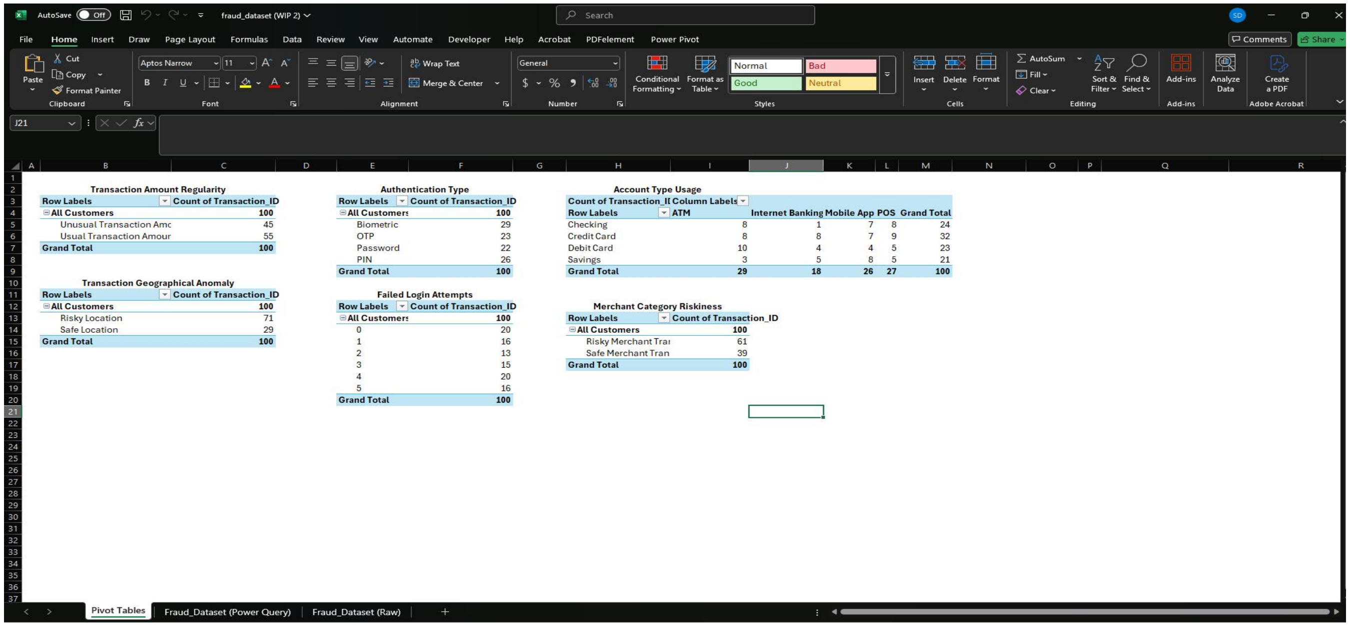
```
= Table.ReorderColumns(#"Added Conditional Column2",{"Transaction_ID", "Customer_ID", "Account_Type", "Channel", "Transaction_Date",
```

	Transaction_ID	Customer_ID	Account_Type	Channel	Transaction_Date	Transaction_Time	1.2 Transaction_
	Valid 100% Error 0% Empty 0%	Valid 100% Error 0% Empty 0%	Valid 100% Error 0% Empty 0%	Valid 100% Error 0% Empty 0%	Valid 100% Error 0% Empty 0%	Valid 100% Error 0% Empty 0%	Valid Error Empty
	100 distinct, 100 unique	46 distinct, 14 unique	4 distinct, 0 unique	4 distinct, 0 unique	78 distinct, 63 unique	99 distinct, 98 unique	100 distinct, 10
1	T0072	C001	Savings	POS	2025-06-02	3:46:00 AM	
2	T0059	C001	Savings	ATM	2025-06-22	12:58:00 PM	
3	T0047	C002	Checking	ATM	2025-05-23	8:01:00 PM	
4	T0048	C002	Checking	ATM	2025-05-20	3:03:00 AM	
5	T0020	C002	Savings	Mobile App	2025-08-17	11:03:00 AM	
6	T0036	C003	Savings	Mobile App	2025-08-25	2:32:00 AM	
7	T0093	C003	Credit Card	Mobile App	2025-03-09	12:09:00 AM	
8	T0022	C003	Debit Card	Internet Banking	2025-02-26	6:52:00 AM	
9	T0063	C003	Credit Card	POS	2025-03-18	2:09:00 PM	
10	T0011	C003	Credit Card	ATM	2025-06-28	10:20:00 AM	
11	T0021	C004	Debit Card	POS	2025-01-12	9:07:00 AM	
12	T0060	C004	Checking	ATM	2025-04-27	1:39:00 AM	
13	T0026	C004	Checking	POS	2025-06-14	4:53:00 PM	
14	T0065	C005	Credit Card	POS	2025-04-27	4:28:00 AM	
15	T0029	C006	Debit Card	ATM	2025-05-15	5:51:00 AM	
16	T0050	C006	Debit Card	POS	2025-01-16	12:14:00 PM	
17	T0034	C007	Credit Card	ATM	2025-03-25	1:30:00 PM	
18	T0040	C007	Checking	Mobile App	2025-06-01	9:24:00 PM	
19	T0071	C007	Credit Card	Mobile App	2025-01-24	12:59:00 AM	
20	T0097	C008	Credit Card	Internet Banking	2025-02-10	3:53:00 AM	
21	T0095	C008	Credit Card	Mobile App	2025-04-28	2:16:00 PM	

Name: Fraud_Datasets

APPLIED STEPS
- Replaced Value3
- Merged Columns
- Filtered Rows2
- Merged Columns1
- Changed Type3
- Removed Columns2
- Added Conditional Column
- Reordered Columns1
- Added Conditional Column1
- Renamed Columns1
- Reordered Columns2
- Added Custom
- Renamed Columns2
- Removed Columns3
- Reordered Columns3
- Renamed Columns3
- Reordered Columns4
- Removed Columns4
- Added Custom1
- Added Custom2
- Added Conditional Column2
- Reordered Columns5

- Pivot tables were generated for possible fraud risk areas for focus



Transaction Amount Regularity

Row Labels	Count of Transaction_ID
⊟ All Customers	100
Unusual Transaction Amc	45
Usual Transaction Amour	55
Grand Total	100

Transaction Geographical Anomaly

Row Labels	Count of Transaction_ID
⊟ All Customers	100
Risky Location	71
Safe Location	29
Grand Total	100

Authentication Type

Row Labels	Count of Transaction_ID
⊟ All Customers	100
Biometric	29
OTP	23
Password	22
PIN	26
Grand Total	100

Failed Login Attempts

Row Labels	Count of Transaction_ID
⊟ All Customers	100
0	20
1	16
2	13
3	15
4	20
5	16
Grand Total	100

Account Type Usage

Count of Transaction_II	Column Labels				
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

Row Labels	Count of Transaction_ID
⊟ All Customers	100
Risky Merchant Trai	61
Safe Merchant Tran	39
Grand Total	100

- Risk metrics (the likelihood and impact) to the risk areas was determined

- Microsoft Power BI dashboard was created to summarize findings

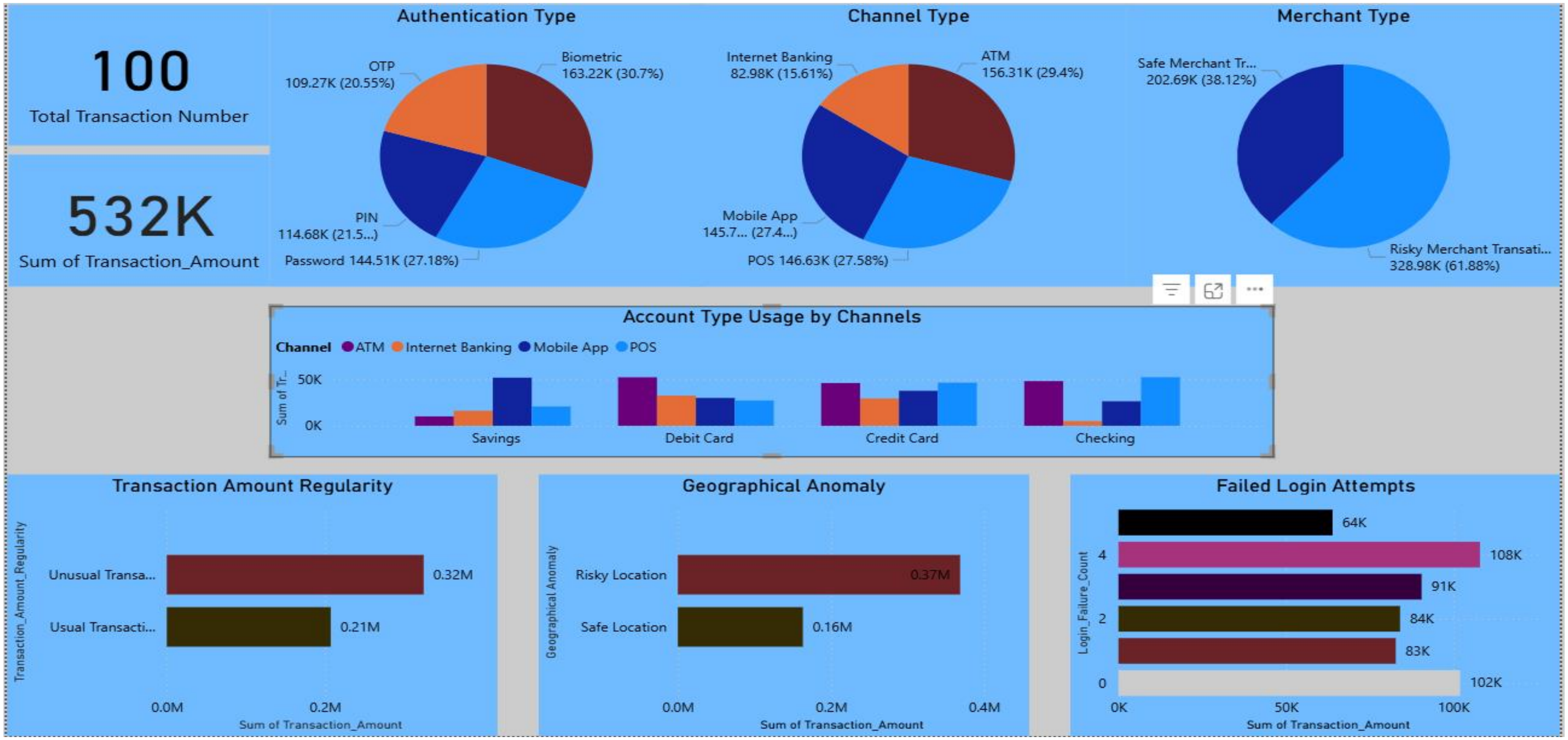
- Recommendations to prevent, detect, and correct identified risk areas using the NIST SP 800-53r5.

2.0 Project Outcomes

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

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

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



Unusual Transaction Amount

The average transaction of each customer is compared to each of the transactions performed by that same customer. Risk is identified where the actual transaction is greater than the average transaction amount for the same customer. 45 transactions were identified as unusual. The total value exposed with this risk is $237,360.61.

Transaction Amount Regularity

Row Labels	Count of Transaction_ID
All Customers	**100**
Unusual Transaction Amount	45
Usual Transaction Amount	55
Grand Total	**100**

Risky Location Transaction

The country of residence was compared to the country of transaction and the authentication type. 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. 71 transactions were identified as risky locations with $368,462.63 exposed.

Transaction Geographical Anomaly

Row Labels	Count of Transaction_ID
All Customers	**100**
Risky Location	71
Safe Location	29
Grand Total	**100**

Risky Authentication Type

Biometric and OTP are more secure authentication than password or PIN. 48 transactions are identified at risk based on authentication type. $259,189.51 I value is at risk.

Authentication Type

Row Labels	Count of Transaction_ID
All Customers	**100**
Biometric	29
OTP	23
Password	22
PIN	26
Grand Total	**100**

Failed Login Attempts

51 transactions with more than 2 failed login attempts are a risk. $262,576.6 worth of transaction is at risk

Failed Login Attempts

Row Labels	Count of Transaction_ID
All Customers	**100**
0	20
1	16
2	13
3	15
4	20
5	16
Grand Total	**100**

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 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 than retail, services, entertainment or food. A customer will highly plan purchases of an electronic or travel expense and will usually perform such transactions from their country of residence. When performed outside the country of residence, there is some level of risk with the transaction. $328,984.62 and 61 transactions are at risk based on merchant category.

Merchant Category Riskiness

Row Labels	Count of Transaction_ID
All Customers	**100**
Risky Merchant Transaction	61
Safe Merchant Transaction	39
Grand Total	**100**

3.0 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 category.

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

Likelihood

Defined as the number of the affected transaction expressed as a percentage to the total number of transactions observed.

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 total amount value of the affected transactions.

Impact Severity	Percentage Referred	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

Risk Category	Likelihood		Impact Severity		Risk Rating	Risk Level
	Percentage	**Rating**	**Amount**	**Rating**		
Unusual Transaction Amount	45%	3	$237,360.61	2	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

Risk Areas Priority and Required Controls

Due to scarce resource and budget constraints, the assessed risk areas must be prioritised as follows 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 Priority	Risk Category	Recommended Controls based on NIST SP 800-53r5
1	Risky Locations Transactions	AC-18: Wireless Access AC-19: Access Control for Mobile Devices AT-2: Literacy Training and Awareness AU-6: Audit Record Review, Analysis and Reporting AU-8: Time Stamps CA-2: Control Assessments CA-3: Information Exchange CA-7: Continuous Monitoring CM-4: Impact Analyses CP-2: Contingency Plan CP-9: System Backup IA-3: Device Identification and Authentication IA-8: User Identification and Authentication IR-8: Incident Response Plan RA-3: Risk Assessment RA-5: Vulnerability Monitoring and Scanning RA-7: Risk Response SC-12: Cryptographic Key Establishment and Management
2	Risky Merchant Category Transaction	
3	Failed login Attempts Risk	
4	Risky Authentication Type	
5	Unusual Transaction Amount	
6	Account Usage Risk	