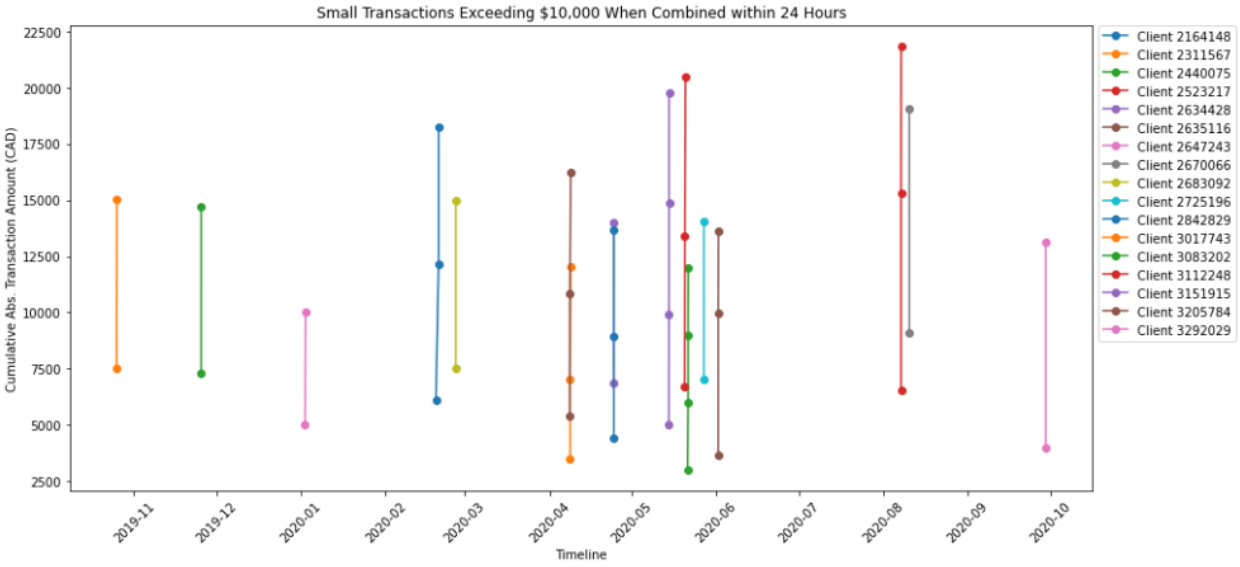
Audit Data Analytics: Reporting EFT-SWIFT Transactions



Contents

A. Introduction and Problem Statement

As a regulatory reporting requirement, certain electronic funds transfers (EFT) through the SWIFT network (EFT-SWIFT transactions) must be reported to the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC). This centre assists in the detection, prevention and deterrence of money laundering and the financing of terrorist activities.

EFT-SWIFT transactions must be reported to FINTRAC if:

- Single EFT-SWIFT transactions exceed $10,000, or
- Two or more EFT-SWIFT transactions (less than $10,000 each) that were made within 24 hours exceed $10,000 in total.

As an auditor, you are required to verify that the audit client reported all EFT-SWIFT transactions timely and accurately. Cases when transactions were not reported timely or accurately need to be presented to the audit client staff for further investigation.

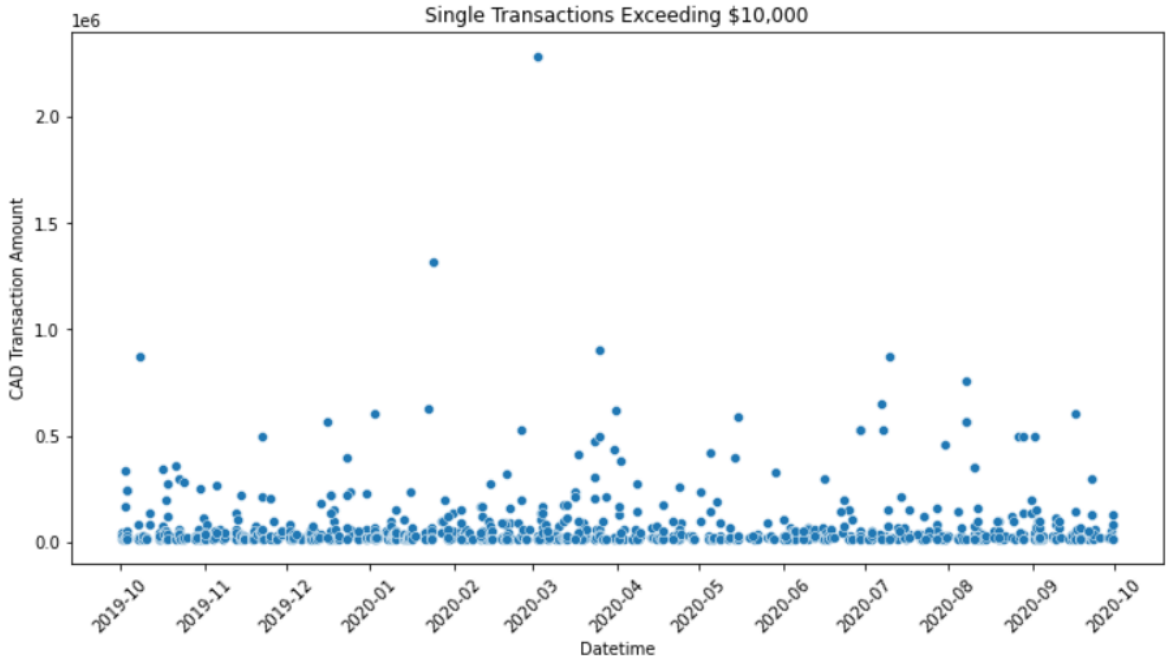
B. Datasets and Exploratory Data Analysis

Two (synthetic) datasets are obtained: one contains raw data for all EFT transactions extracted from the admin system for the audit period and one contains transactions that were reported to FINTRAC during the audit period.

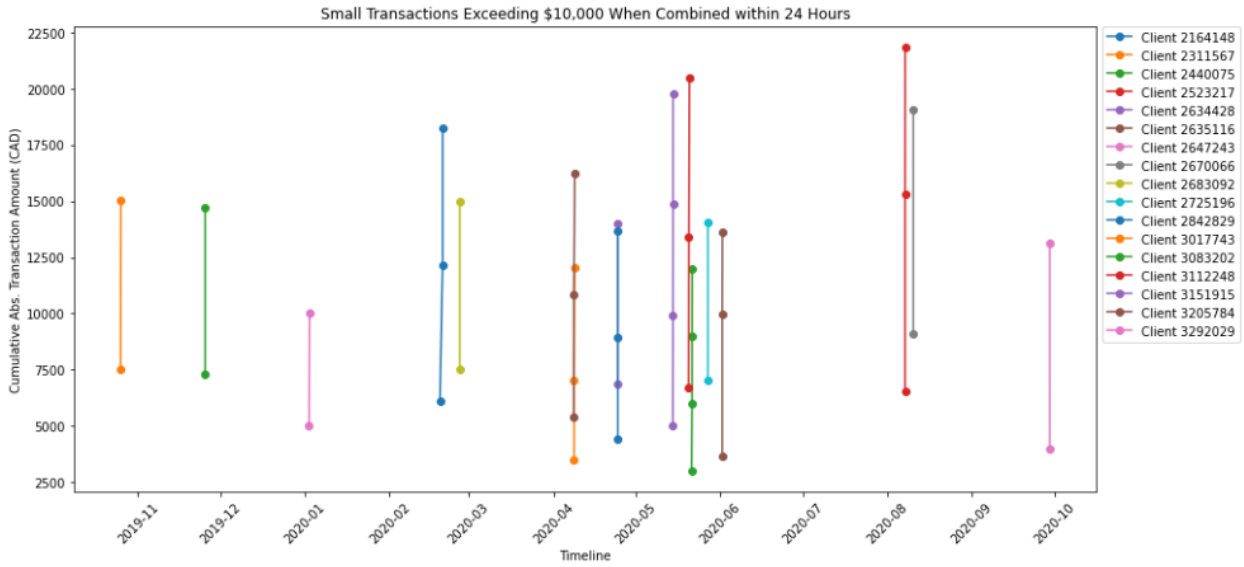
The following observations and assumptions were made as the datasets were explored.

- The audit period is between October 1, 2019, and September 30, 2020, as evidenced via the range of ‘EFFECTIVE_DATE’ in the raw dataset.
- The ‘EFFECTIVE_DATE’ of the raw dataset is supposed to be the transaction date. In the reported dataset, the transaction date is in the data field ‘Tran Date’.
- The ‘Filing Date’ of the reported dataset is the reporting date.
- The ‘TRANSACTION_CODE’ of the raw dataset can be mapped to the ‘Report Type’ of the fintrac_reported dataset as {‘DM’: ‘EFTO’, ‘CM’: ‘EFTI’}. In other words, debit memos correspond to EFT out, and credit memos do EFT in.
- ‘TRANSACTION_AMOUNT’ of debit and credit memos can have positive sign or negative sign, depending on the nature of the transaction (e.g., reversal transactions have amounts in opposite signs to the original transaction amounts).
- The ‘CIF’ (standing for Customer Information File) of the raw dataset is the ‘Client ID’ of the reported dataset.
- Regarding ‘CIF’: All the 48,093 distinct CIF numbers in the audit period have 7 digits except for three CIFs: 0, 55713, and 950799 that have less than 7 digits. Inquiries about these unusual CIFs with the audit client will be help understand more about them. What if they are data quality issues?
- 18 Client IDs in the reported dataset are not in the raw dataset. These are from transactions between July 30, 2019, and September 30, 2019, outside the audit period.

- There are no common single unique data fields that can be used to map transactions between the two datasets. Thus, data mapping for two-way matching requires more thoughts.
- There are no missing/null values in the data records.
- There are quite a few large transactions with amounts greater than $500,000, as illustrated in the scatterplot.



- 17 clients had transactions with amounts less than $10,000 each but exceeding $10,000 in cumulative total within 24 hours. This is extracted from the results of my algorithm.



C. Analytics Approach and Reasoning

I come up with the following audit data analytics approach to verify that the audit client reported all EFT-SWIFT transactions timely and accurately.

Step 1: Devise suitable algorithms to find, from the raw dataset, EFT-SWIFT transactions that must be reported to FINTRAC and that satisfy the conditions given. Then implement the algorithms in Python code. This will independently give me the EFT-SWIFT transactions to validate and reconcile with the transactions reported to FINTRAC.

Step 2: Given no common single unique data fields between the raw dataset and fintrac_reported dataset, use combinations of applicable existing data fields to enable the data mapping / transaction matching between the two datasets.

Step 3: Given the results of Step 1 and Step 2, devise and implement the test scenarios using Python.

- Scenario 1: Test that the audit client has reported EFT-SWIFT transactions timely among the transactions reported by comparing between the 'Filling Date' and 'Tran Date'. Save the transactions not reported timely to csv for further investigation. Please be noted that this Scenario 1 can be done without the Step 1 and Step 2.
- Scenario 2: Test that the audit client has reported EFT-SWIFT transactions accurately by matching the transactions reported with the corresponding EFT-SWIFT transactions in the raw dataset and by comparing the reported transaction dates and amounts with the raw dataset. Additionally, check if any transaction in the reported dataset is not in the independent list of must-report EFT-SWIFT transactions obtained in Step 1. Save exceptions to csv for further investigation.
- Scenario 3: In addition, test that all the must-report EFT-SWIFT transactions obtained in Step 1 were already reported to FINTRAC. Cases where must-report EFT-SWIFT transactions from Step 1 are not noted in reported dataset will be saved to csv for further investigation.

These scenarios will not only help to verity that EFT-SWIFT transactions reported to FINTRAC are timely and accurately but also help verify reporting completeness.

Additional Assumptions While Implementing the Approach

I base on the following additional assumptions. It is important that these assumptions be confirmed with the audit client. Revisions to analytical steps can be made if confirmed differently.

- Only international wire transactions with transaction descriptions in 'International Wire', 'US International Wire', 'REV International Wire', 'International Wire BoC', and 'REV International Wire BoC' are considered EFT-SWIFT transactions. This is important for Step 1.
- 'US International Wire' transactions in the raw dataset have transaction amounts in USD. Conversion to equivalent CAD amounts is necessary to compare the converted amounts to the threshold of $10,000.

- I use the average USD/CAD rate of 1.3457 after averaging the daily FX rates provided by BoC for the audit period to convert the USD transaction amounts to CAD.
- Since transaction amounts in the raw dataset have different signs, their absolute values are used to compare with the threshold of $10,000 for both single transactions and cumulative total transaction amount of two or more EFT-SWIFT transactions.
- The algorithms that I coded to find single EFT-SWIFT transactions and two or more EFT-SWIFT transactions that were made within 24 hours (less than $10,000 each but total to $10,000 or greater) and that must be reported to FINTRAC are assumed to be correct. These algorithms show that 938 EFT-SWIFT transactions must be reported to FINTRAC in the audit period. These transactions are used to perform two-way matching with the EFT-SWIFT transactions reported to FINTRACT in the fintrac_reported dataset.
- Reversal EFT-SWIFT transactions are included, and their absolute transaction amounts can be added to the cumulative sum. They are not used to net-off with the original transactions.
- The combination of 'CIF', 'EFFECTIVE_DATE', 'TRANSACTION_AMOUNT' (Absolute), and 'TRANSACTION_CODE' in the raw dataset and the combination of their counterparts ('Client ID', 'Tran Date', 'Tran Amt', and 'Report Type') in the reported dataset enables transaction matching between the two data sets if the matched transactions have the same transaction dates and amounts.
- The combination of 'CIF', 'TRANSACTION_AMOUNT' (Absolute), and 'TRANSACTION_CODE' in the raw dataset and the combination of their counterparts ('Client ID', 'Tran Amt', and 'Report Type') in the reported dataset enables transaction mapping between the two data sets if the transactions have different transaction dates but the same transaction amounts.
- Where the raw data has transaction amounts to the hundreds or not to the units, if the matched transactions in the fintrac_reported have the amounts rounded to the units, it is considered inaccurate reporting in the fintrac_reported dataset.
- Transactions reported in the reported dataset but not in the audit period are out of scope and are excluded.

D. Audit Data Analytics Testing Results

- 762 out of 771 EFT-SWIFT transactions reported to FINTRAC in the audit period between October 1, 2019, and September 30, 2020, were not reported timely as the filing date is different from the transaction date (see the csv file "not_timely.csv" for the detailed listing).
- 228 EFT-SWIFT transactions reported to FINTRAC have transaction amounts rounded to the nearest units for reporting instead of preserving the original amounts. This can be considered inaccurate reporting (see the csv file "rounded_transaction_amounts.csv" for the detailed listing) although the transaction dates are accurate.

- 72 EFT-SWIFT transactions reported to FINTRAC have reported transaction dates different from the raw data and the reported transaction amounts rounded to the nearest units instead of preserving the original amounts in the raw data (see the csv file “different_tran_dates_and_rounded_amounts.csv” for the detailed listing).
- 13 EFT-SWIFT transactions reported to FINTRAC are not in the list of EFT-SWIFT transactions generated by the algorithms. There are potential inaccuracies in reporting these transactions. Further investigation with the audit client is needed (see the csv file “not_part_of_algorithm_results.csv” for the detailed listing).
- 1 EFT-SWIFT transaction (report ref EFTO2019100300001001) reported to FINTRAC does not match any transactions in the raw data.
- 2 EFT-SWIFT transactions (report refs EFTI2019112500001002 and EFTO2020030200001004) reported to FINTRACT have inaccurate amounts reported but not due to normal rounding errors.
    - EFTI2019112500001002: reported amount is $53,842 while the raw data transaction amount is $53,841.06 (if rounded, it would give $53.841)
    - EFTO2020030200001004: reported amount is $61,370 while the raw data transaction amount is $61,368.76 (if rounded, it would give $61,369)
- 167 out of 938 must-be-reported EFT-SWIFT transaction records generated by my algorithms are not found in the EFT-SWIFT transactions reported to FINTRAC (see the csv file “must_report_transactions_not_in_fintrac_reported.csv” for the detailed listing).

In conclusion, not all EFT-SWIFT transactions were reported timely and accurately in the audit period from October 2019 to September 2020. There is also risk of incomplete reporting according to the last bullet point. Please consider the audit observations noted in the bullet points above and their associated detailed listings for further investigation.

E. Python Code

Please find the Python code and supporting comments in the Jupyter notebook on GitHub at https://github.com/alexphamcpa/audit_data_analytics/blob/main/EFT%20Transactions/ADA_Reporting_EFT_SWIFT_Transactions.ipynb

.