Team FinHack

NBS BAC x Deloitte Business Analytics Hackathon 2022

Nanyang Business School

Deloitte.

01

The Scope

Prevalence of Fraud

Context: Possible existence of Internal and External Fraud pointed out by whistleblower that individuals related to the banks are using accounts payable, employee expenses and corporate credit cards to fraud the company.

Problem Statement: These Frauds are allegedly easy to execute and may cost the company greatly in the long run as financial and reputational risks are involved.

Strategic defrauding through objectives

Key objectives:

- To analyze the datasets given on accounts payable, corporate credit cards and payroll with inter-dataframes comparison resulting in identification of ghost and duplicated employees accounts

- Highlight possible fraudulent transactions and individuals with suspicious activity with visualization across countries through geospatial data to track discrepancies in cash outflow

- Quantify current fraudulent transactions with strategic outline of impacts and recommend solutions to deter such problems in the future to result in tailwinds for efficient fraud management

Common Fraud in the Market

Credit Card

1. Fictitious expenses
2. Mis categorization of expenses
3. Duplicate expenses
4. Non-arm's length expenses

Payroll

1. Ghost Employee Fraud
2. Advance Retention Fraud
3. Pay Rate Alteration Fraud
4. Compensation Fraud

Account Payable

1. Check Fraud
2. Expense Reimbursement Fraud Schemes
3. Over Billing
4. False Billing
5. Duplicate Invoice Pyament
6. Pass-through schemes
7. Disguised Personal Purchases
8. Fake Vendor

02

Interpretation and Risk Profiles

Risk profiles

The data given has been subset into 3 distinct categories, with key fraud identification towards Internal, External and Internal-to-External Stakeholders and Cashflow direction. The various datasets and utilizations are outlined as follows:

Internal-to-External	Internal	Internal-to-External
Dataset: Accounts Payable.XLSX	**Dataset:** Payroll.XLSX	**Dataset:** Credit Card Data.XLSX
• Expense Reimbursement Fraud (Duplicated report submission) • Billing Fraud (Falsified Billing information)	• Ghost Employee Fraud • Pay Rate Alteration Fraud • Unauthorized Employee Fraud • Fake Vendor Fraud	• Fictitious expenses • Mis categorization of expenses • Duplicate expenses • Non-arm's length expenses

03

Analytical Process Flow

Analysis Process

Shortlist Potential Frauds

List potential frauds identifiable from the given data.

Data Cleaning

Clean data to ensure easier and consistent analysis

Data Exploration

Explore data to identify potential frauds listed previously.

Quantify Cost

Quantify cost of fraudulent activity found.

Data Visualisation

Visualisation for clarity and presentation

Devise Solutions

Create long-term solutions to deter the identified fraudulent activity in the future.

04

Data in analysis and Limitations

Data used in analysis

Payroll Data:

- Employee Master & Pay slip sheets

Credit Card Data:

- Leave & Transactions sheets

Accounts Payable Data:

- Invoice and Vendor Master sheets

Limitations

- No documentation of data (Data Dictionary unavailable)
- Lack of several confidential employee information (E.g. names to identify if employee has promoted since employee id changed from XXXXXX to XXXXXA)
- Missing vendor and employee information (Inability to reconciliate data across datasets and join tables)

05

The Team’s Analytical tools

Analytical Tools

R

- Accessible for everyone (Open-Source Programme)
- Ability to use data frame, SQL, statistical tools for analysis
- A Large Variety of Libraries & cross-platform support.
- Potential to build machine learning models to prevent fraud through predicting factors that result in fraud

SQL

- Easy to understand & use
- Structures and data are kept very safe as it is not easily changed.
- Can be used within other programming language like R and Python (Interchangeable IDEs)
- Good for extracting data for comparison

Analytical Tools

Tableau

- Tableau is one of the most commonly visualization tool
- Highly accessible and easy to learn
- Multiple functions for dashboarding and storytelling

06

Key Insights

Outcomes from Data Mining and Analysis

Accounts Payable: Billing Fraud

False Billing occurs when employees or accounts are created for invoices for goods and services that were either not delivered, or payment were taken for the individuals themselves. A qualitative comparison of geospatial data in Address and Country reflected anomalies in Billing Information, where the postal code and country reflected were different. For example, the address could be '8591 Corona St. New Albany, IN 47150', yet country receiving the payment would be Singapore.

A Qualitative Analysis of the Payments by Geographical location is as follows:

Qualitative Comparison of Postal Codes in Address and Country in billing information reveal disparities in location, illustrating that cash outflows reached areas highly related to Terrorism and Tax-Sensitive areas, such as Iraq and Americas respectively.

Regions denoted in Countries graph shows areas that could be in Lumbago Edge Bank's Scope, such as Asia and Australia, as they are headquartered in Singapore with operations in Malaysia. Excess transactions per regional basis could show layering and placement of cash in Anti-Money Laundering.

Accounts Payable: Expense Reimbursement Fraud

Expense Reimbursement fraud results in fictitious payments for items that were never purchased. or expenses that may be overstated to external vendors or external accounts.
The team identified several key insights as follows, from the Accounts payable Excel Database, Invoice Sheet:

Unique Accounts in Flow transaction vendors: 233

Total duplicated entry count: 814

Duplicated Accounts in Flow transaction vendors: 125

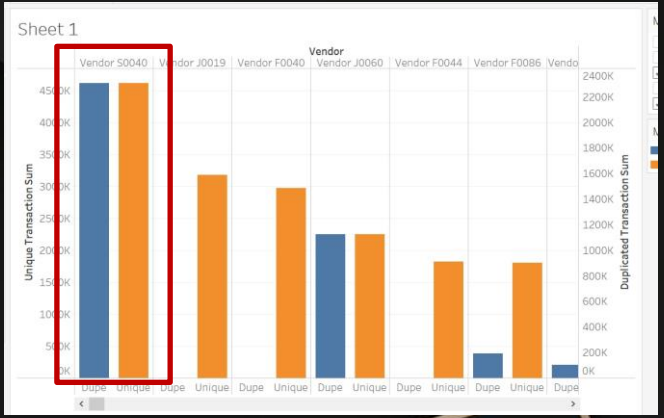
Sum of Unique Flow Transaction: SGD$ 29,947,931 (Non-duplicated transaction)

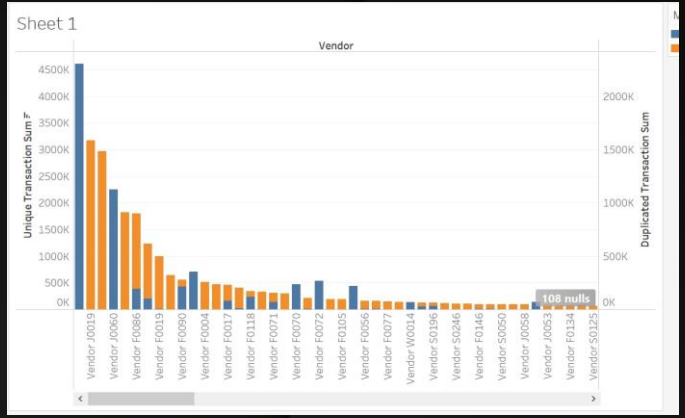
Sum of Duplicated Flow Transaction: SGD$ 6,079,815 (Duplicated transaction)

Thus, from the insights, we were able to deduce that more than **50% of Vendor accounts (53.65%)** for transactions were repeated in duplicated transactions, while **16.88% of total transactions** were duplicated in the invoices. The accounting discrepancies and fictitious payments can signal possible money laundering within the bank involving external transaction accounts.

Accounts Payable: Expense Reimbursement Fraud

The team further investigated the data based on percentage overstatement of the transaction flow figures (in SGD$) relative to actual transactional details (Unique data that appeared once). The top 6 vendors for percentage overstatement and duplicated transaction sum are as follows:





With reference to Vendor S0040, it is alarming as although its percentage overpayment is 50%, the duplicated transactional sum that has been overpaid is **SGD$2,306,389.** Another anomaly is Vendor NBSZ **(SGD$352,238.6 overpaid , 68.56% overpaid)** which appears in the Payroll fraud, where the employee's bank account was disguised as a vendor, showing statistical correlation of Fraud.

Payroll: Ghost Employees

Ghost Employees are non-existent employees entered into the payroll where another employee receives income from. In this section, 3 key identifiers of each employee is looked into to highlight potential ghost employees.

Bank Account

Highlighted Employee IDs:

- 0020186 & 020186A
- 0038776 & 0454690

Mobile Number

Highlighted Employee IDs:

- 0020186 & 020186A
- 0038776 & 0454690

Home Phone

Highlighted Employee IDs:

- 0064264 & 0064265
- 0037981 & 0240513
- 0038389 & 0038412
- 0037057 & 0037935
- 0036630 & 0036675
- 0034964 & 0038562
- 0023791 & 0042009
- 0052468 & 0052992

Payroll: Ghost Employees

Bank Account and Mobile Number highlighted the same potential ghost employees. Further analysis was done on the payslips to identify if these employees have been drawing salaries at the same time.

Duplicate Pair 1: 0020186 & 020186A

While the employee IDs may suggest that it may be a promotion with an added "A" following the 1st ID, no salary pay-outs were found to this pair.

Duplicate Pair 2: 0038776 & 0454690

This pair highlighted salary pay-outs to both employees during the same period. While one of them is Daily-Paid and another is Monthly-Paid, employees with multiple salary forms are usually paid to a single account.

Payroll: Ghost Employees

Home Phone was analysed under the assumption that one can have multiple bank accounts & mobile phone number but people tend to have only one home phone, provided it is a requirement for the payroll employee to enter into the master.

8 Duplicate Pairs

As Home Phone is not a concrete proof that these may be ghost employees, more information is required for this analysis.

Therefore, there is concrete evidence highlighting **0038776 & 0454690** as a ghost employee while further investigation is required for the 8 duplicated home phone employees. Quantifying the cost of the ghost employees, if:

0038776 is the ghost employee: $121,208

0454690 is the ghost employee: $763.05

Payroll: Pay Rate Alteration Fraud

Pay Rate Alteration Fraud occurs when an employee with access to the payroll system alters the pay rate for some employees. In this case, since there are no hourly-paid employees, monthly changes is highlighted for further investigation.

1539 Employees have highlighted a net total change in their salary pay-out. This costs $60,736,531 with a change as high as $208,659.26 for a single employee.

577 Employees have highlighted a net total change in their BASIC salary pay-out. This has cost Lumbago $10,405,655 with a change as high as $110,087.50 for a single employee.

Changes in net total salary pay-out may contribute to other factors such as bonuses, commissions and allowances while net changes in basic salary may be due to raises. Therefore, more information and further investigation is required to ascertain fraudulent activity.

Payroll: Unauthorised Employee Fraud

Unauthorised Employee Fraud occurs when an employee that should not have been paid is receiving a salary pay-out. In this case, contractual employees are investigated if they are paid beyond the end of their contract.

Control: 30 Days beyond contract end date is used as a criterion to provide buffer for last-month salary crediting.

Number of Employees Paid Beyond 1 Month After Contract ends: 215

Total Cost for Unauthorised Employees: $10,675,226.24

With the lack of information, the number and cost of unauthorised employees is alarming and should require further attention.

Payroll: Fake Vendor Fraud

Fake Vendor Fraud occurs when an employee purchases from an entity owned or connected to them, possibly charging for the product/service above market value resulting in a conflict of interest.

6 Vendors have been highlighted with their bank account belonging to an employee in the employee master.

Of which 3 Vendors have the same bank account number as the Ghost Employee Pair (0038776 & 0454690).

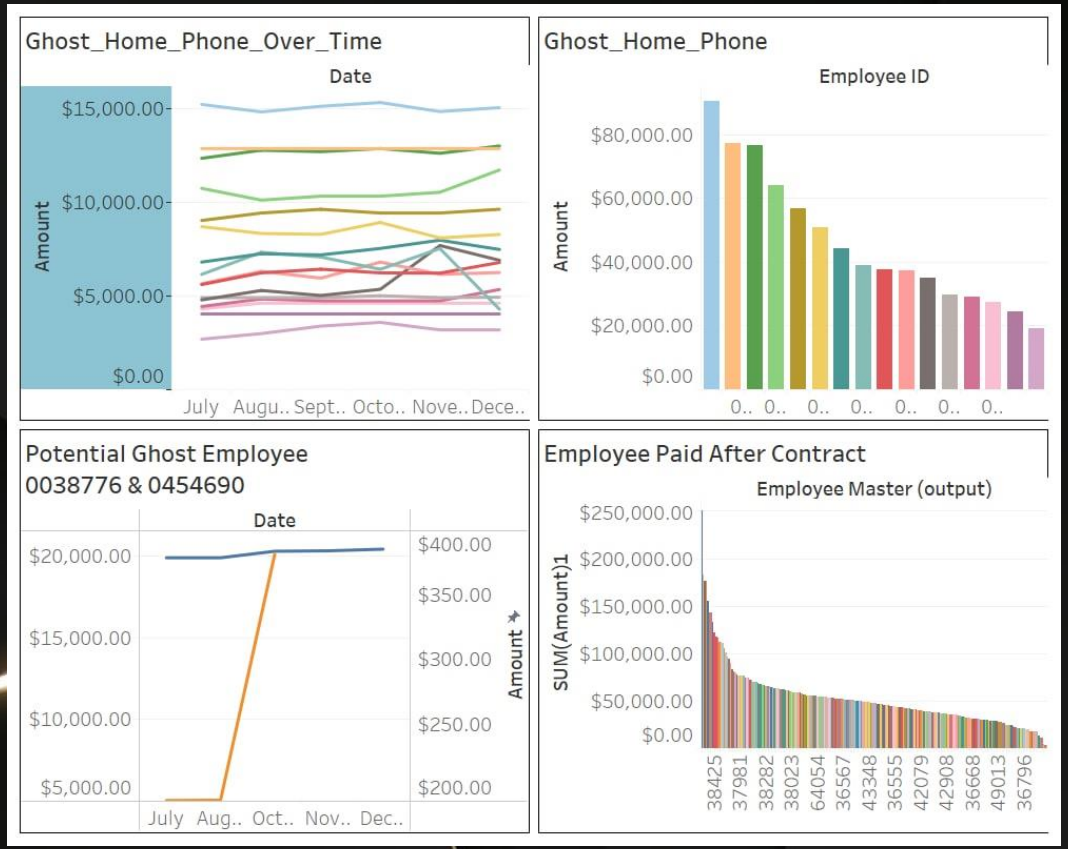
No recent payments have been made to these vendors.

Other 3 Vendors have 2 distinct bank accounts, both receiving recent payments.

2 Fake Vendors had cost Lumbago Edge Bank:
F0086: $2,340,342
NBSZ: $1,744,018

Therefore, the 2 fake vendors had claimed large amounts of money from Lumbago Edge Bank, and NBSZ has been highlighted in the Expense Reimbursement Fraud Analysis as well.

Cost of Payroll Frauds to Lumbago



Credit Card: Duplicate Transactions

Duplicate expenses. Seeking reimbursement more than once for the same expense.

3524 instances where duplicated transactions were found for credit card transactions. The duplicated transactions amount to $418,477.7 and involved multiple employees as well as vendors.

Number of Employees involved in duplicated transactions: 401

Number of Vendors involved in duplicated transactions : 568

103 instances of unsubmitted claims for credit card transactions were also present. These unsubmitted claims involved 31 vendors.

Due to the massive number of duplicated transactions, there is a high chance that employees may be making multiple claims for one expense. The employees and vendors involved should be investigated to find out if there was collusion among the two parties.

Credit Card: Personal Expenses

Occurs when employees use corporate credit card on their personal expenses. To identify such instances of fraud, it is assumed that spending done during their leave represents irrelevant expenses.

894 instances of credit card spending was done during leave days. The suspected personal expenses amount to $268,567.39 and involved multiple employees.

Number of Employees involved in Personal Expenses: 320

While there is a high number of employees seemingly using the corporate credit card during the leave days, the limitations to the dataset require additional inquiry into this fraud. The lack of transaction time and the inadequate information on corporate culture (working on leave) may void these instances as fraud.

07

Recommendations

Remediations and Resolutions

Minimising Billing Fraud Occurrence

Monitoring of payment transfers to regions out of geographical operations to prevent layering and placement of cashflows in Anti-Money Laundering. This increases accountability and operational trade outflows for the Bank

Counter-terrorism financing should also be noted, and respective countries should be on the blackout list of the Bank, as **qualitative analysis showed that there were payments made to the Iraqi region, despite the country being recorded as Philippines.**

In the Geospatial data, we can see that the discrepancies between cashflows sent by Postal codes and Countries included countries such as the Americas and European region. However, the scope of Lumbago bank is headquartered in Singapore with Operations in Malaysia. Hence, **large payments to western countries could be deemed as red flags.**

This is important as Anti-Money laundering can lead to negative effects such as reputation loss to the Bank, where in a reputational risk study of 49 reputation-related events by Professor Walter of New York University, negative cumulative abnormal returns of up to 7% and US$3.5 billion were found.

Negating Expense Reimbursement Fraud

With 16.88% of Total flow dollars being duplication transactions, this is alarming for the bank as it is over $6 million and rectification of the transactions (reversal of expenses) from external vendors will be labor-consuming and challenging to overcome, as the geospatial data shows that expenses have been submitted and transferred to areas of high risk and terrorism.
To overcome this issue, the team has outlined three methodologies that Lumbago Bank can employ in process automation and limit losses on expense reports:

Tighten Approval Processes with Automation and AI

- Only 32% of companies automate links between expense reports and process claiming
- Require all finance outbound processes to require multiple authentication. (Integrate expense, subscription, procurement and invoices

Implement use of Corporate card with greater control

- Query each card individually and transaction and ensure that payments are being made against them.
- Review credit activity reports on a monthly basis from issuing company.
- Compare credit activity to determine excessive transaction to unknown vendor and transaction location

Formal review process and routinely question expenditures

- Managerial individuals or special AML department set up to review employee reports, expense to perform cursory reviews frequently.
- Routinely question expenditures that look extradordinary (large amounts or duplicated transactions with large percentage difference)

Deterring Internal Payroll Fraud

Tighten Approval Processes with Machine Learning/AI

- Use of Machine Learning to identify possible anomalies for further investigations.
- Require all finance outbound processes to require multiple authentication.
- E.g. Approval of payslips/entering employees into payroll system require payroll staff approval → Machine Learning System → Manager/Director Approval

Limit Vendor Through Partnerships

- Securing partnerships with limited vendors.
- Allow expense reimbursement only from limited vendors.
- Regular audit/review of vendors – including credit review of vendors
- E.g. Specific clinics, hotels and suppliers.
- This ensures that there are no conflict of interest with vendors and the regular review ensures financial survivability of suppliers.

Fixed Payment

- GIRO/SWIFT set-up to remit fixed payments to certain bank accounts
- Prevents double crediting to the same account
- Prevents pay rate alteration due to fixed amounts.
- Ensures efficiency of payment process.

Credit Card Fraud Prevention

Revise spending and claims policies

1) Limit the amount of expenses that can be submitted without receipts
2) Place limits on certain activities per person such as meals and entertainment
3) Put in place strict penalties for those who violate the polices

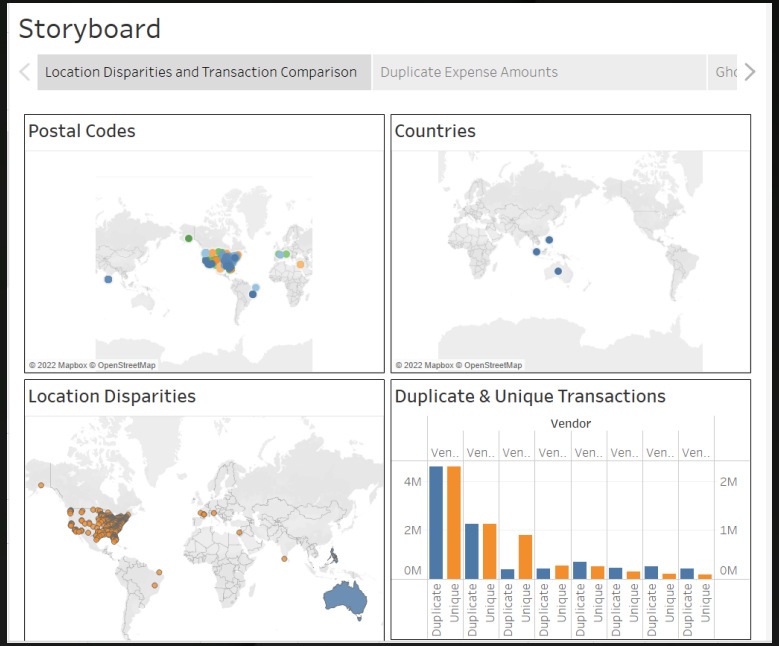
Intensify audits & Reviews

1) Utilize AI or machine learning techniques that can identify fraud and examine outliers to validate spending
2) Reviewing the company credit card statements and expense reports for accuracy
3) Get managers to review receipts and expenses report before submitting them for claims

References

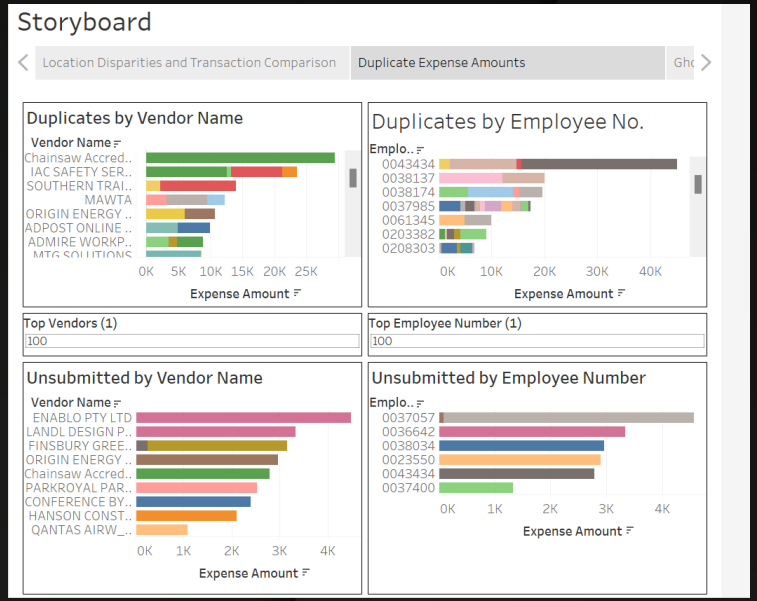
- https://www.stampli.com/blog/accounts-payable-fraud/types-of-accounts-payable-fraud/
- https://bestaccountingsoftware.com/accounts-payable-scams/
- https://thepaypers.com/expert-opinion/trust-is-hard-to-gain-but-easy-to-lose-a-banks-reputation--1249891
- https://www.forbes.com/sites/edwardsegal/2020/12/14/how-to-guard-against-corporate-credit-card-and-expense-report-fraud/?sh=3650b8d7f85f
- https://www.stpaulschambers.com/most-common-types-of-payroll-fraud/
- https://www.accountingtools.com/articles/types-of-payroll-fraud
- https://stonebridgebp.com/library/uncategorized/expense-reimbursement-fraud-ten-ways-to-protect-your-organization/
- https://blog.spendesk.com/en/expense-report-process

Appendix: Storyboard of Location Disparities and Transaction Comparison



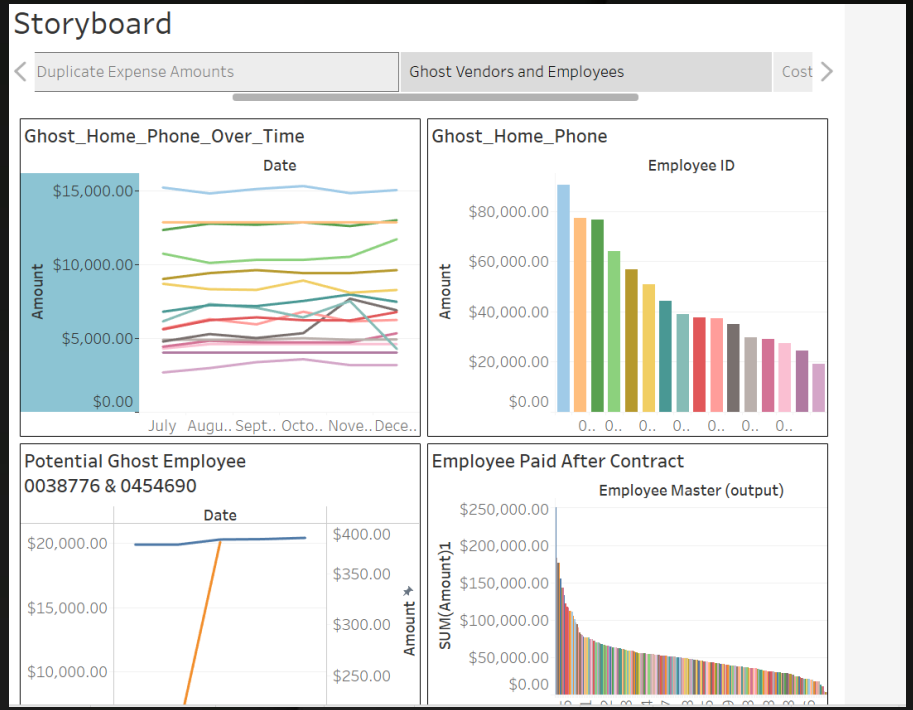
Source: Tableau File Storyboard sheet

Appendix: Storyboard of Duplicate Expense Amounts



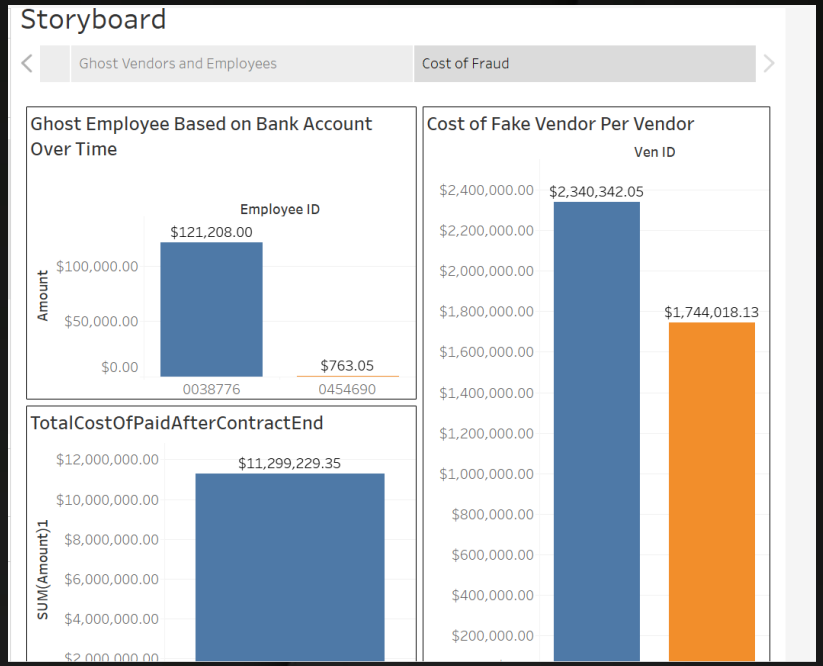
Source: Tableau File Storyboard sheet

Appendix: Storyboard of Ghost vendors and Employees



Source: Tableau File Storyboard sheet

Appendix: Storyboard of Cost of Fraud



Source: Tableau File Storyboard sheet