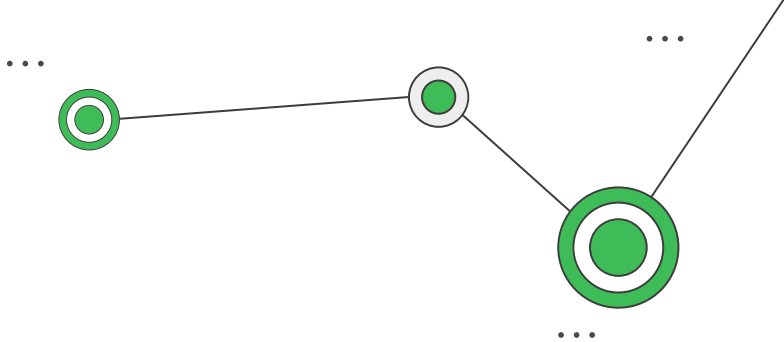
Deloitte.

VSLAM analytics



Lumbago Edge Bank

Investigating Fraud Utilising Advanced Analytical Techniques

NBS BAC Hackathon

VSLAM

Ananya Balehithlu | Bai Shun Yao | Max Tan Zheyuan

Tan Kit Hon, Luke | Vinay Krishnaa Vinod

Table of Contents

01
Scope

Situational Analysis & Our Interpretation

Situation:

Whistleblower Fraud Accusation

Cause:

Unsatisfactory current salaries

Effect:

- Alleged 'Defrauding'
- Involving accounts payable, employee expenses and the use of corporate credit cards.

Interpretation

Due to financial constraints and ease of defrauding, employees might engage in fraudulent activities in order to ease their financial struggles

Approach

Utilising advanced analytics techniques, comb through accounts payable, expenses and credit card transaction data to identify suspicious activities that render financial advantages to employees

→ **Develop Risk Profiles**

Scope | Data Exploration | Risk Profiles | Recommendations | Laundering Detection

02
Data Exploration

Assumptions & Limitations

Accounts Payable Data

- Vendor: Without information as to when vendors have been "deactivated" or "discontinued", we assumed that no transactions to these vendors have ever been approved.
- Invoice: Other than November 2021, where data is missing, the remainder of all invoices have been accurately recorded.
- Payment: No payment is made before an invoice is issued.

Credit Card Data

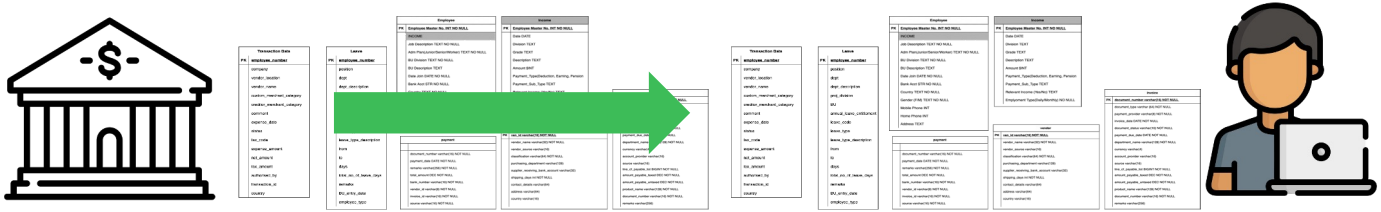
- Transaction Data & Leave:
  - Assumed no system error (e.g. duplicated information was manually inputted)
  - Assumed nature of transaction ID (e.g. must be unique & numeric)
  - Assumed that some columns were not mandatory to fill in (e.g. comments)

Payroll Data

- Employee Information
  - Assumed lack of personal particulars is unintentional negligence (missing/duplicate addresses, numbers)
- Payslips
  - Assumed ordinary earnings for each employee remain largely similar through the 6-month period
  - Assumed pensions to employees are outflows while deductions from employees are inflows of cash

Workflow

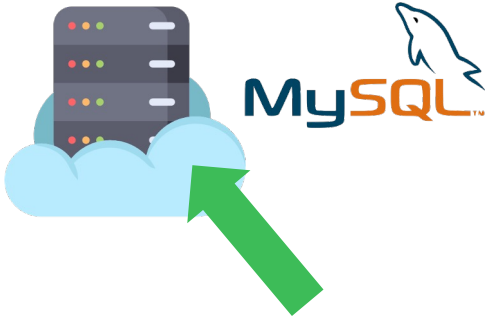
From the Bank

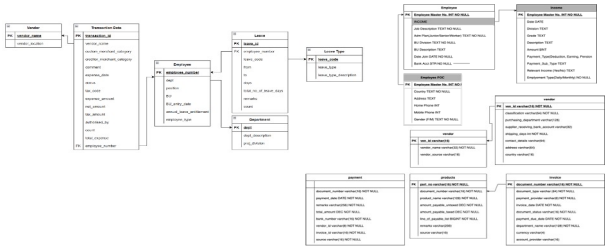


Scope | Data Exploration | Risk Profiles | Recommendations | Laundering Detection

Workflow

Migration



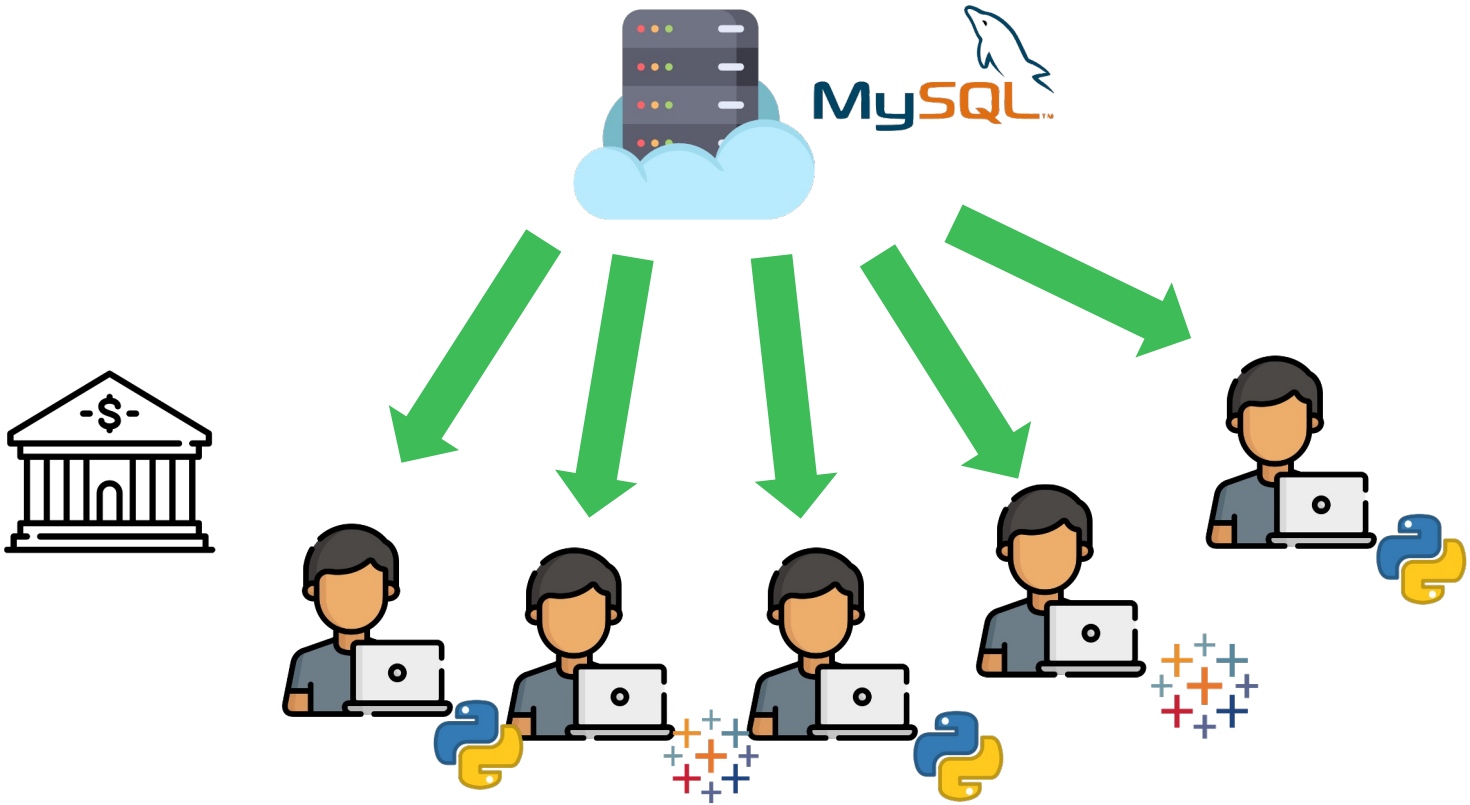


R Studio

Scope | Data Exploration | Risk Profiles | Recommendations | Laundering Detection

Workflow

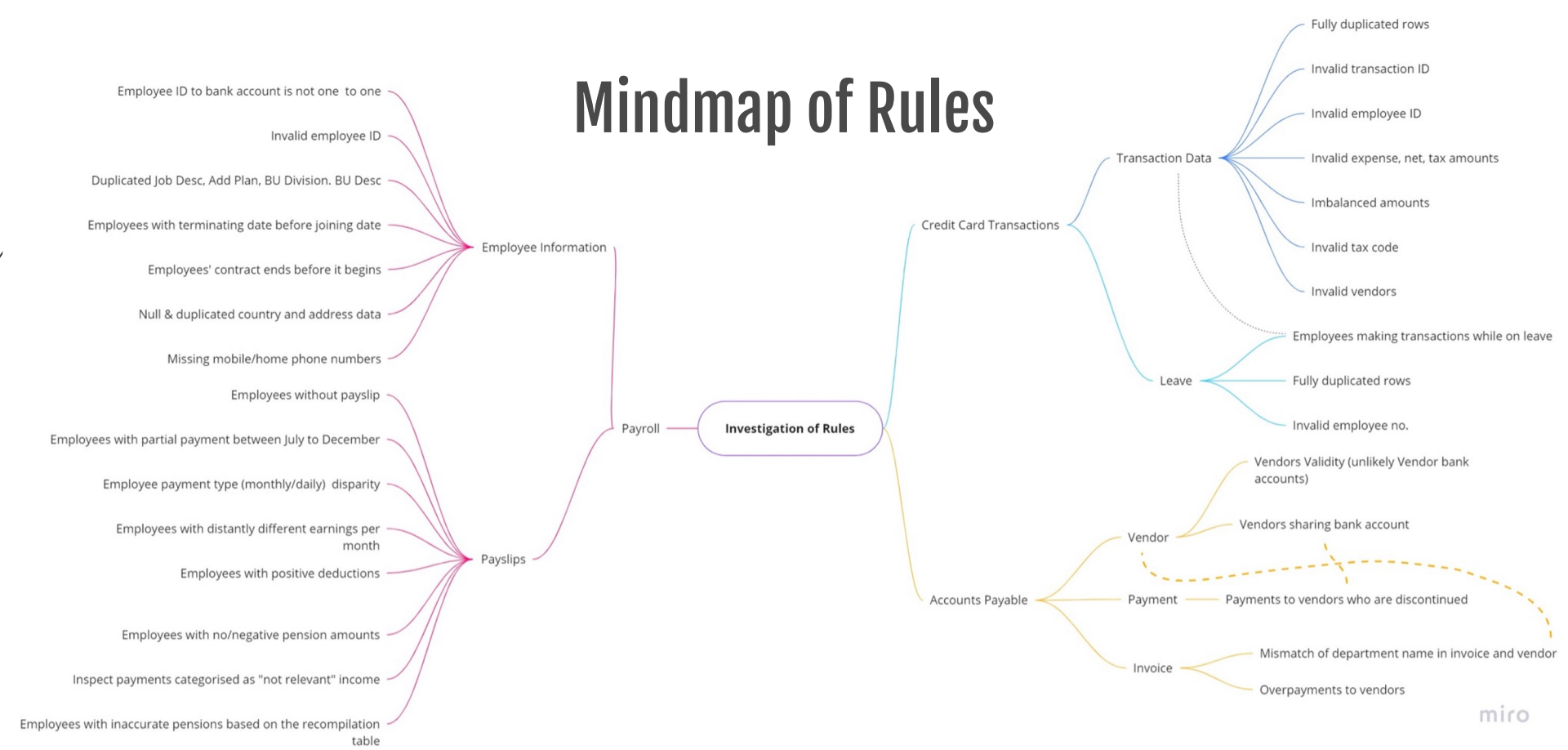
Analysis Process



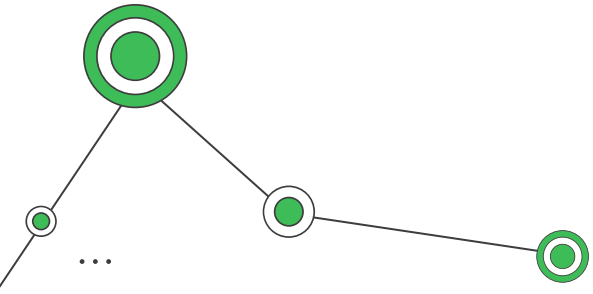
Scope | Data Exploration | Risk Profiles | Recommendations | Laundering Detection

03
Risk Profiles

Mindmap of Rules



Scope | Data Exploration | Risk Profiles | Recommendations | Laundering Detection



Risk Profiles

Disruptive Actors

Invalid entries

Ghost Actors

Fake employees/vendors

Malicious Actors

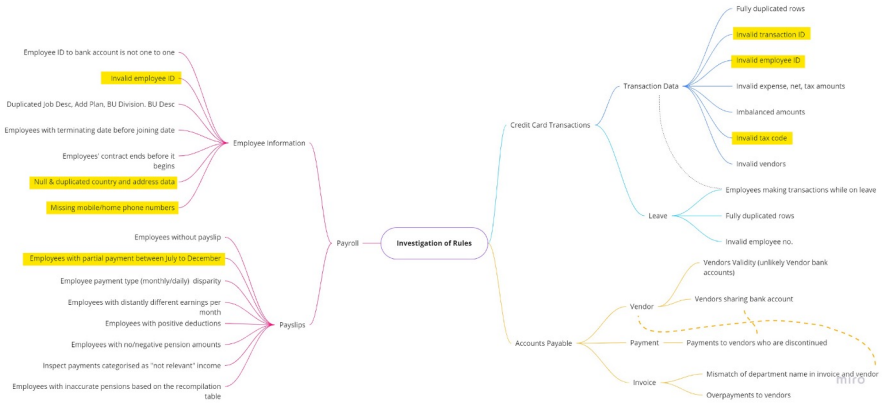
Insiders with malicious intent

Disruptive Actors

People who make invalid entries.

Proposed Rules

1. Invalid transaction IDs (Credit Card)
2. Invalid employee numbers (Credit Card)
3. Invalid tax codes (Credit Card)
4. Invalid/missing employee particulars (Payroll)
5. Deviations in ordinary payments (Payroll)



Disruptive Actors

Summary of Findings

Total Amount Lost
$ 4,717,165.12

17.4%

Number of Suspected Actors
1277

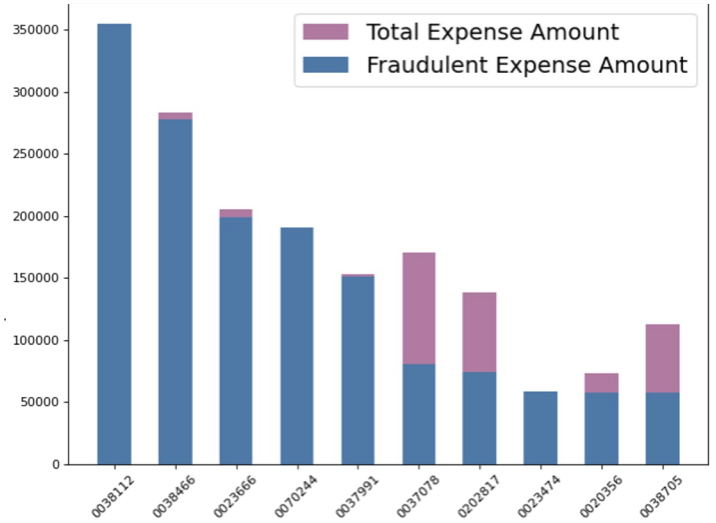
Most Prominent Rule

Invalid Transaction IDs

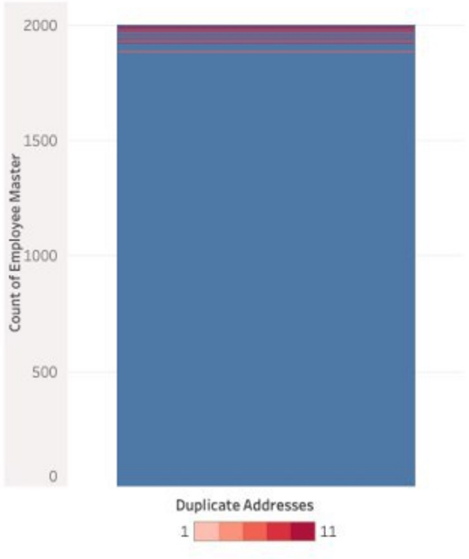
1276 employees committing fraud caught

Implementing rule prevents significant loss

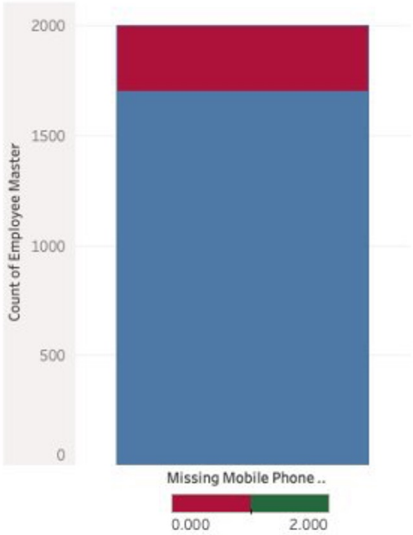
Top Perpetrators with invalid Transaction IDs



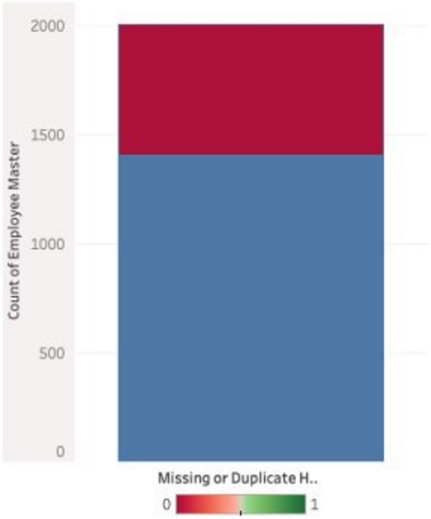
Duplicate or missing Address Fields



Invalid or Missing Mobile Phone Numbers

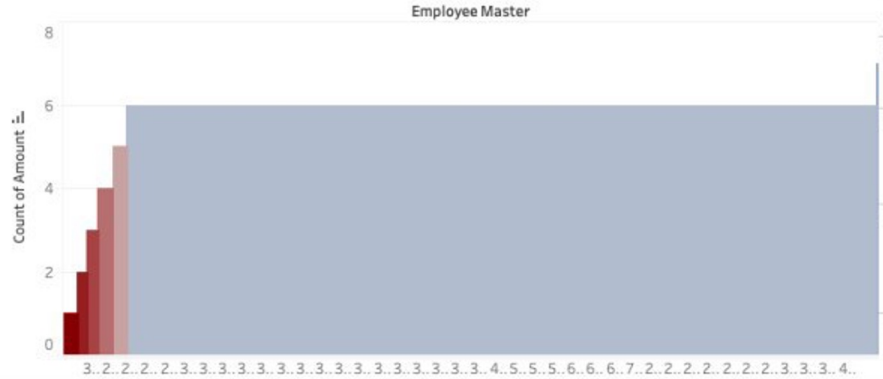


Invalid or missing Home Phone Numbers



Snapshot of Tableau Dashboard for Disruptive Actors

Number of ordinary salary payslips per employee



Employee Number

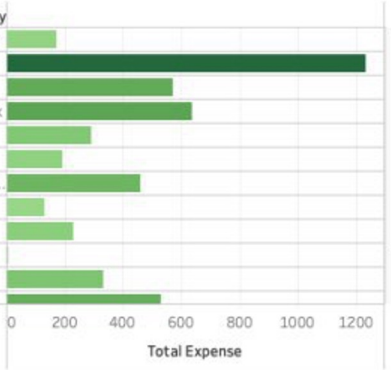
(Multiple values)

Total Expense

7 1,232

Invalid Employee Numbers

Employee Number	Transaction..	vendor name (Transactio..	Custom Merchant Category
020186A	42536	DATAWORLD PTY LTD	Telephones and Fax Office
	SR139620	FINSBURY GREEN PRNTIN..	Stationery
	SR144043	FINSBURY GREEN PRNTIN..	Stationery
0020305	12390	DOCUMENT DYNAMIX	Minor Equipment Under 5k
	210951	BALLINA SHIRE COUNCI	Unknown
	225184	OFFICE EXPRESS	Stationery
	CHHP7974	J BLACKWOOD & SON P/L	Repairs & Maintenance Eq..
0021364	12597539	246000 FCMTRAVELSOLUT	Travel Domestic Airfares
		VIRGIN AUST	Travel Domestic Airfares
	12605721	246000 FCMTRAVELSOLUT	Travel Domestic Airfares
		QANTAS AIRW_ABN1600..	Travel Domestic Airfares
		REGIONAL EXPRESS RSP	Travel Domestic Airfares

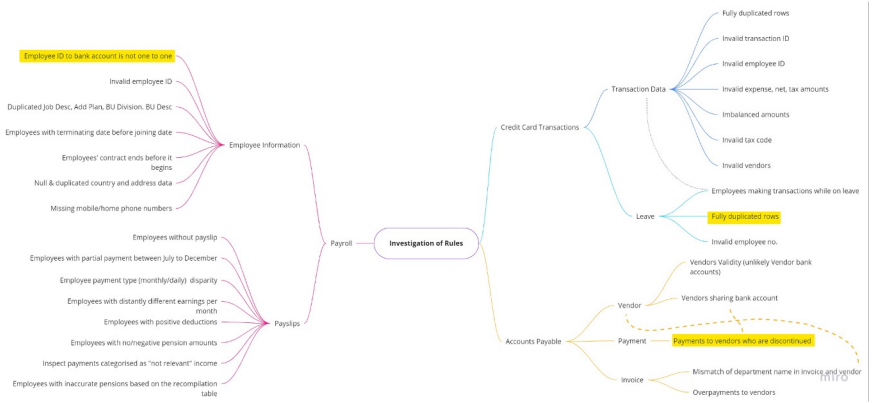


Ghost Actors

People not part of the organisation

Proposed Rules

1. Duplicate rows (Credit Card Data)
2. Fake vendors (Accounts Payable Data)
3. Employees with matching bank accounts (Payroll Data)



Ghost Actors

Summary of Findings

Total Amount Lost
$ 219,542.84

Number of Suspected Actors
1,325

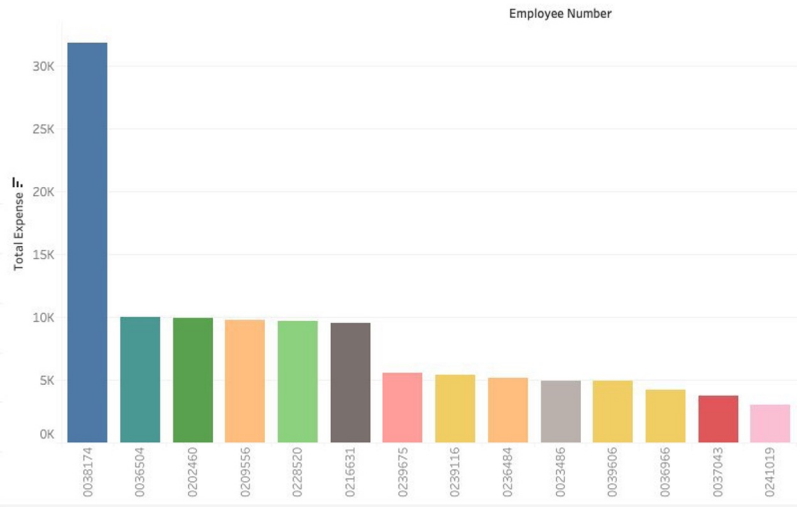
Most Prominent Rule

Duplicate Rows in Credit Card Data

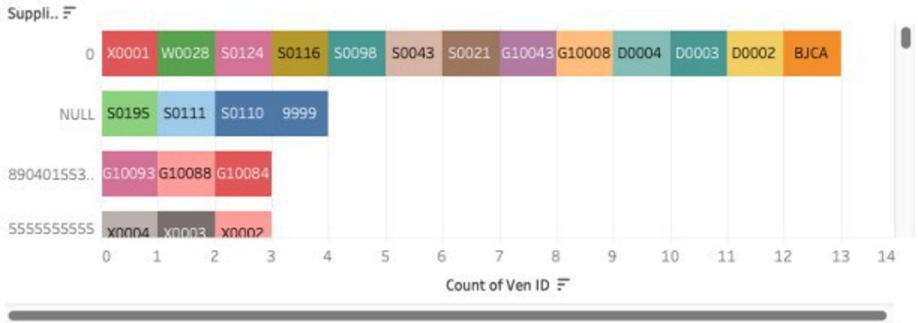
Rows that are 100% alike in all attributes are indicative of invalid/unauthorised transactions.

The same transactions are charged multiple times. This could indicate cash flow to dummy actors

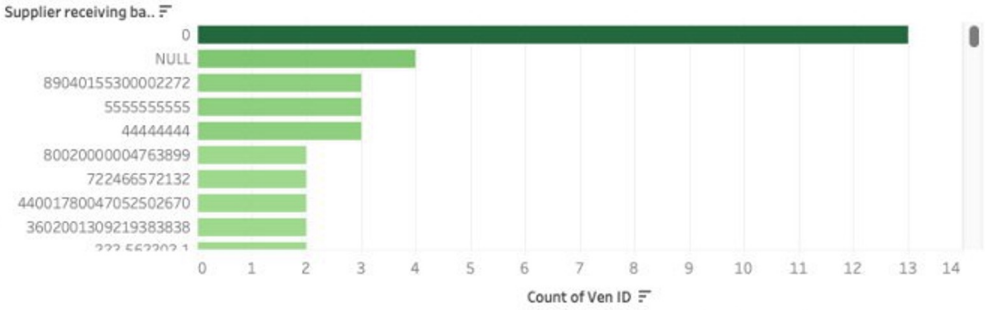
Total expense amount for duplicated rows



Unlikely vendor bank accounts



Number of occurences of bank accounts

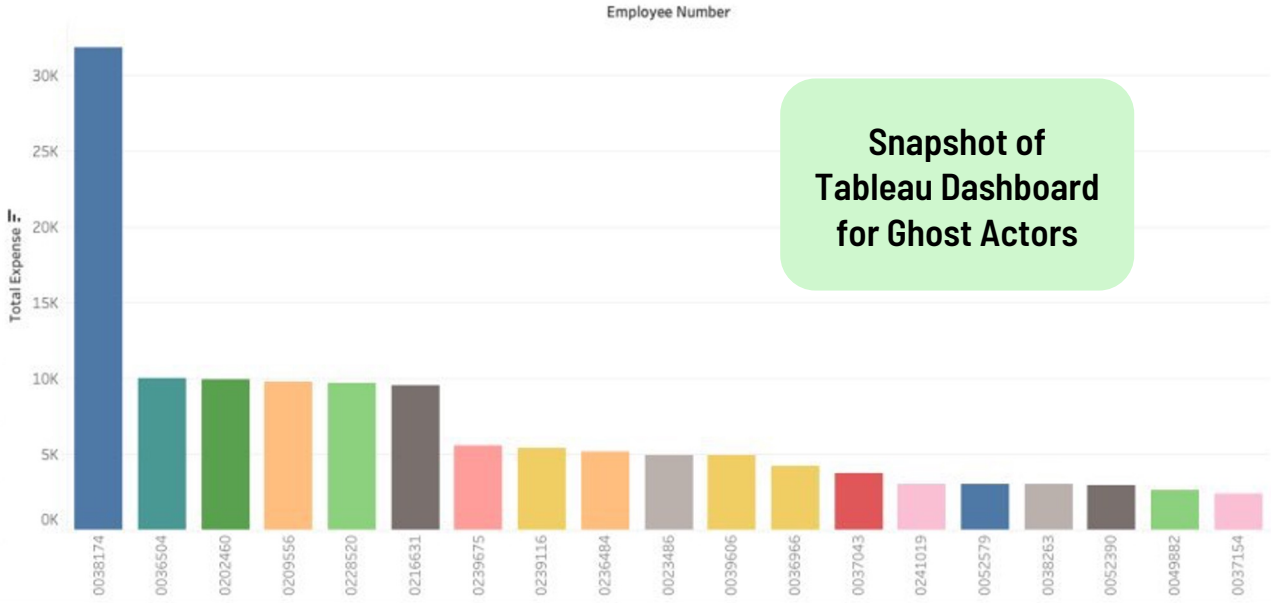


Employees with matching Bank Accounts

Employee Master (..	Bank Acct	
Null	282-8803243	Abc
20186	282-8803243	Abc
38776	5555555555	Abc
454690	5555555555	Abc

Total value of duplicated rows

Total expense amount for duplicated rows

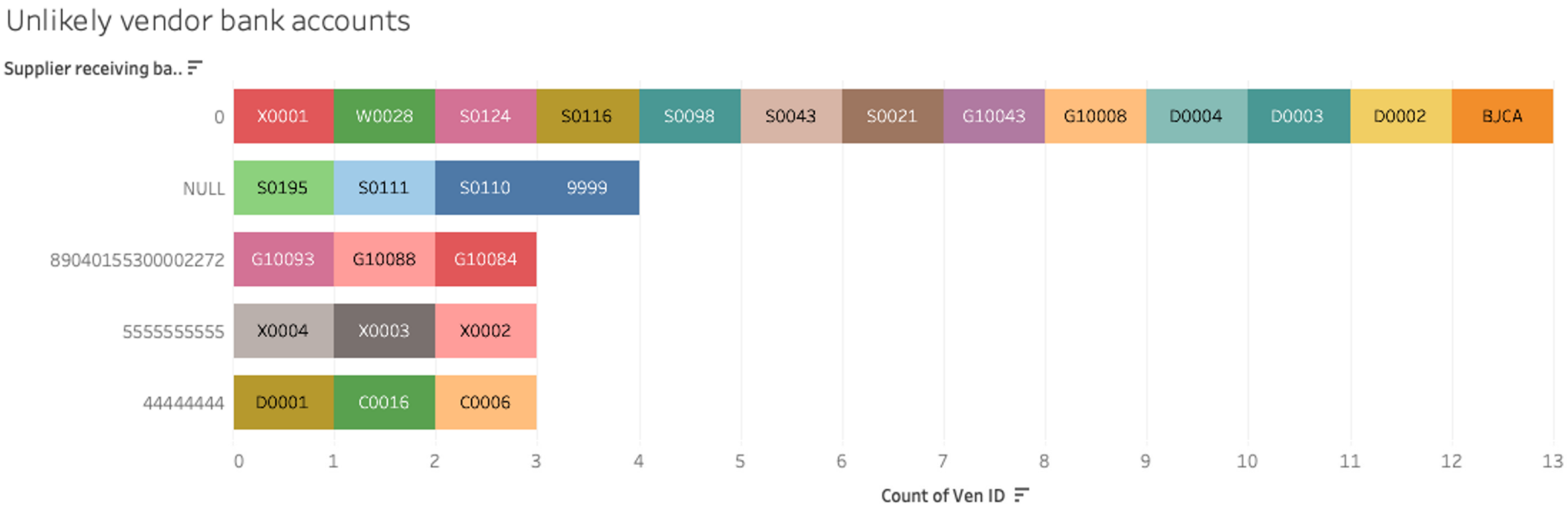


Snapshot of Tableau Dashboard for Ghost Actors

Ghost Actors

Unlikely Vendor Bank Accounts

Some vendors have unlikely bank accounts listed,
suggesting that money could have been siphoned away as false payments.

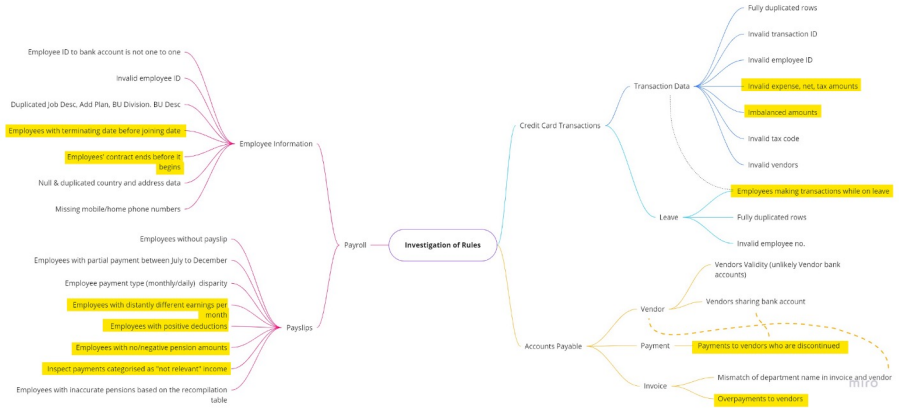


Proposed Rules

1. Employees making transactions during leave (Credit Card)
2. Negative amounts (Credit Card)
3. Amounts should tally with each other (Credit Card)
4. Payments to discontinued/deactivated vendors (Accounts Payable)
5. Overpayments to vendors (Accounts Payable)
6. Embezzlement by ex-employees (Payroll)
7. Particular performance grade has abnormally high salary (Payroll)
8. Deductions recorded as cash outflows (Payroll)
9. Pensions recorded as cash inflows (Payroll)
10. Large payments recorded as "not relevant" income (Payroll)

Malicious Actors

Employees abusing authority



Malicious Actors

Summary of Findings

Total Amount Lost
$17,558,122.6

Number of Suspected Actors
2,484

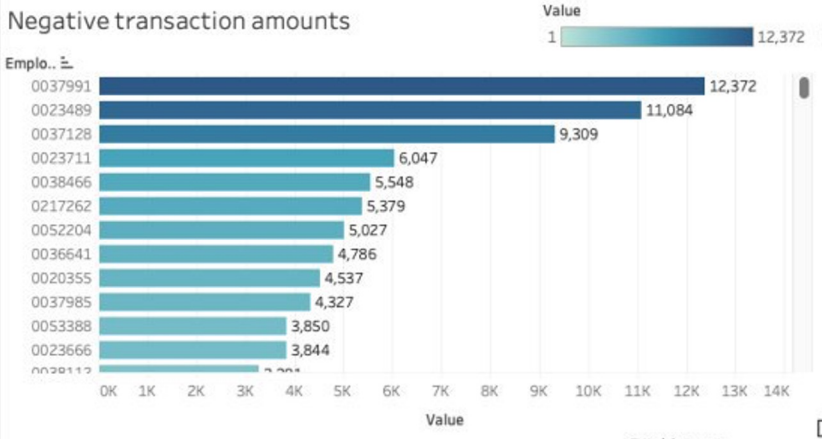
Text Mining Approach

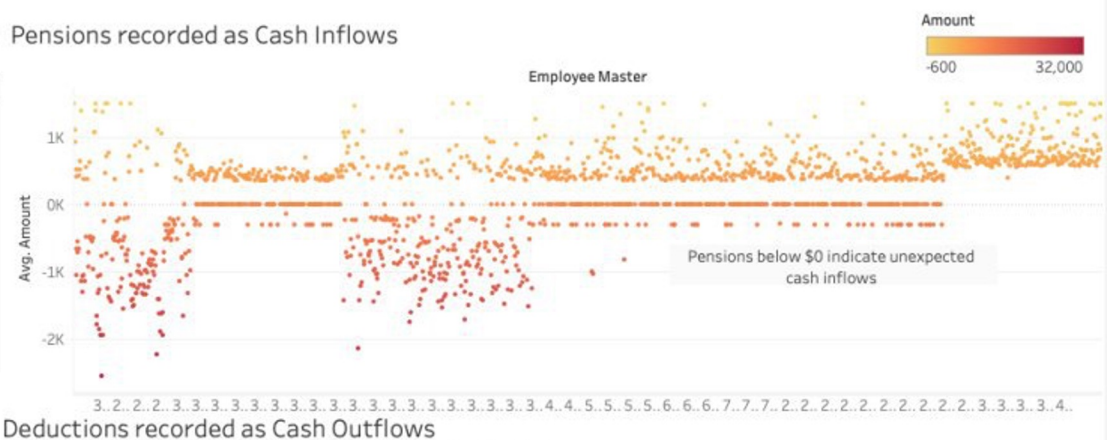
Negative values in transactions are dangerous as they could hide fraudulent amounts transacted

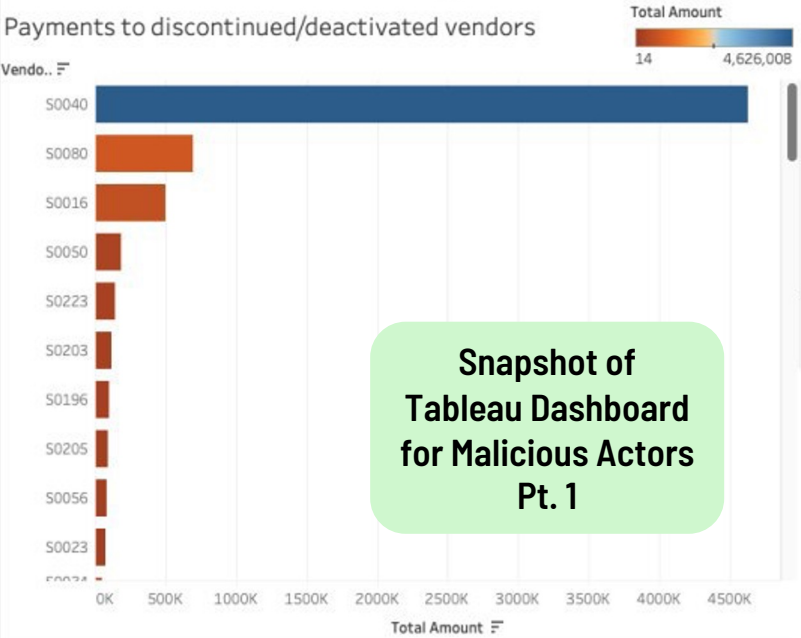
However, upon closer inspection, there is a need to check if transaction is a refund or reimbursement → legitimate transactions

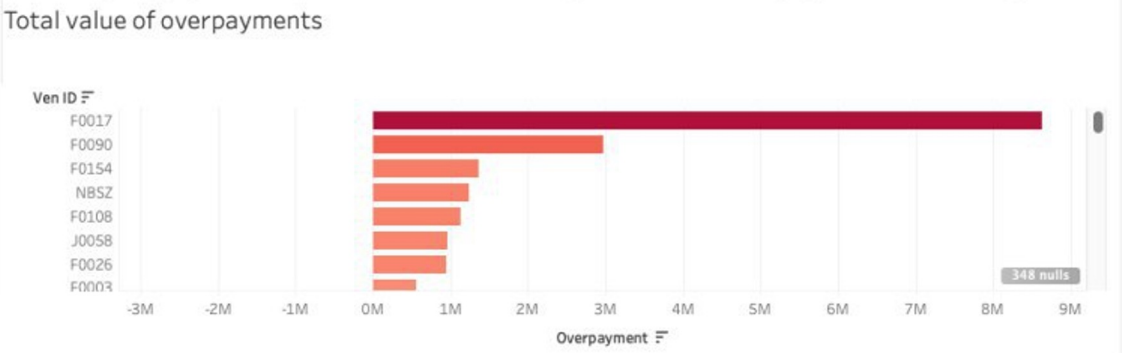
Text Mining on "comment" column to eliminate legitimate negative amount transactions

After filtering refunds and returns, remaining transactions that have negative expenses are considered suspicious. This fraud results in the company incurring more expenses than reflected

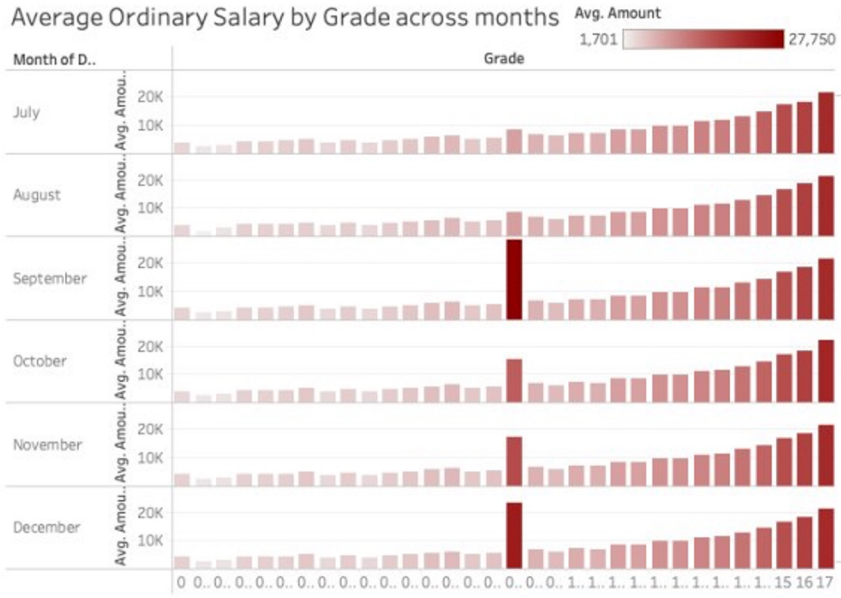


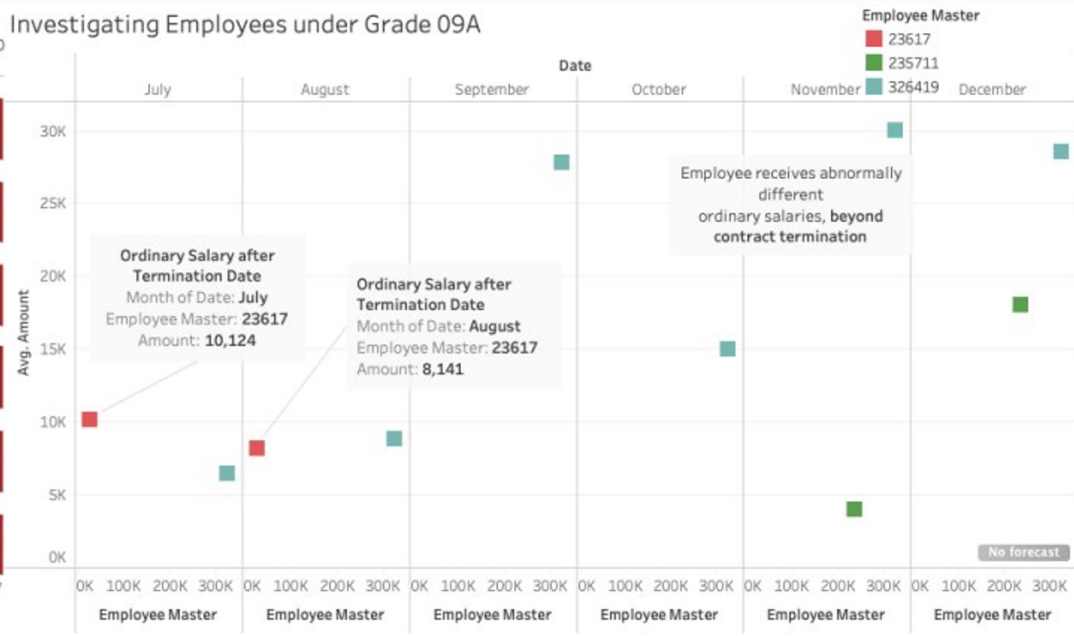


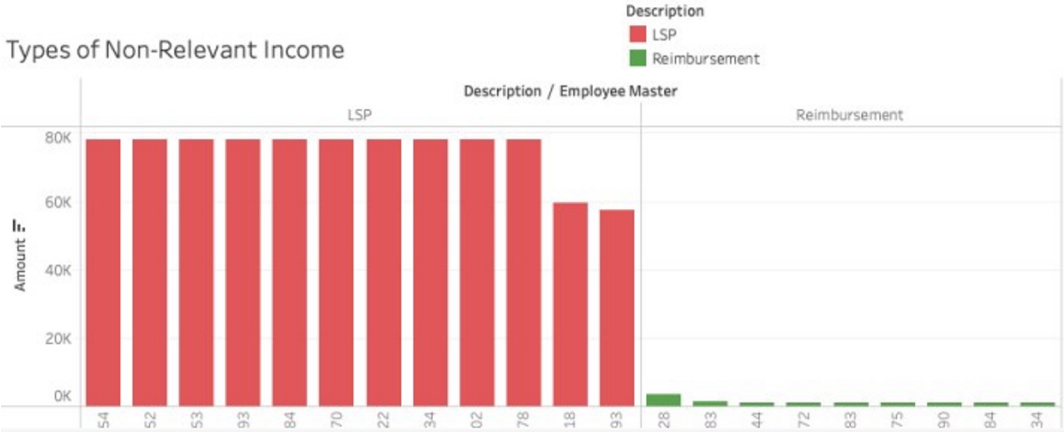


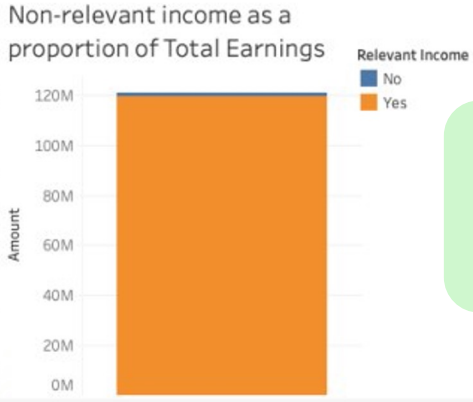


Snapshot of Tableau Dashboard for Malicious Actors Pt. 1

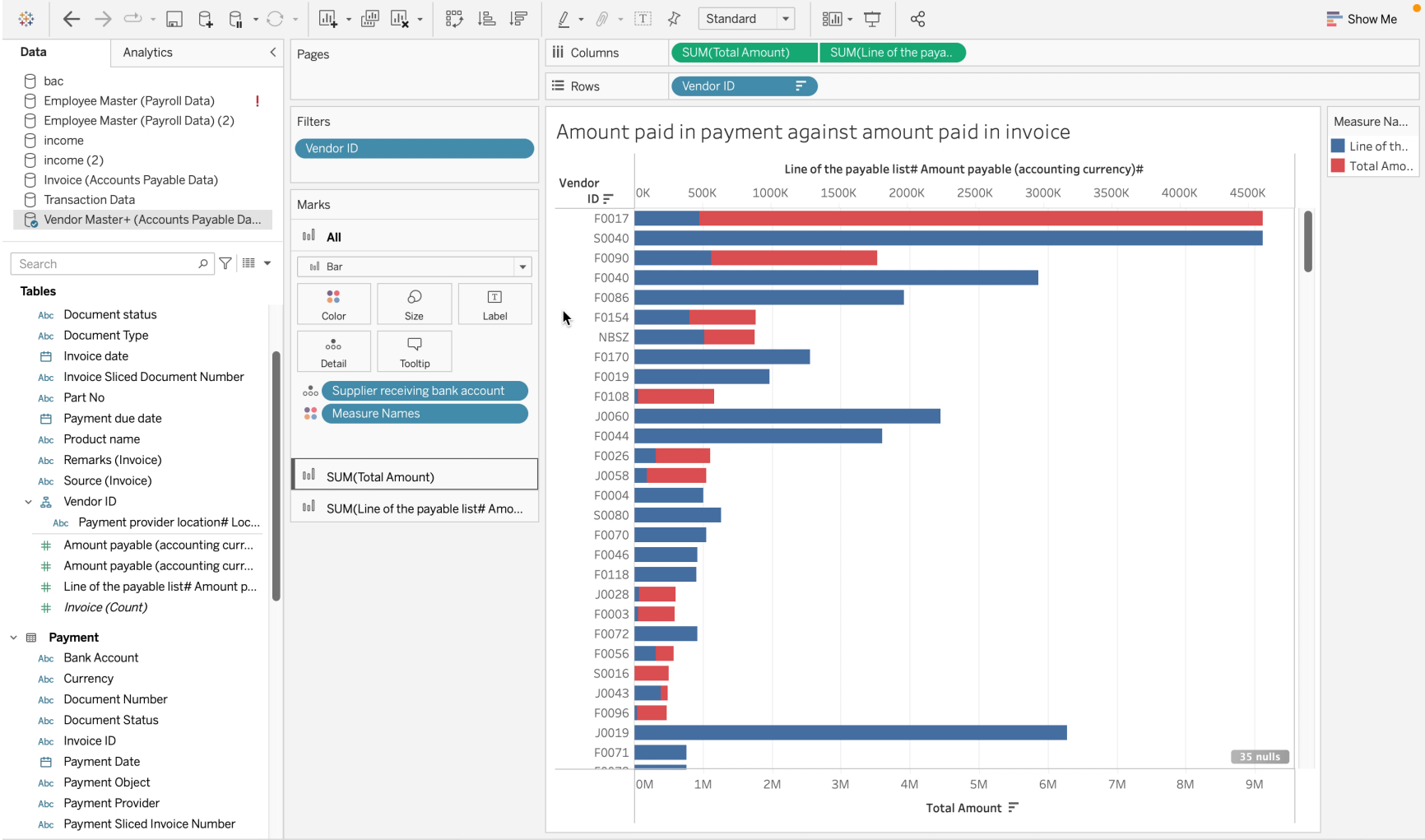








Snapshot of Tableau Dashboard for Malicious Actors Pt. 2


Standard
Show Me
Data
Analytics
bac
Employee Master (Payroll Data)
Employee Master (Payroll Data) (2)
income
income (2)
Invoice (Accounts Payable Data)
Transaction Data
Vendor Master+ (Accounts Payable Da...
Search
Tables
Document status
Document Type
Invoice date
Invoice Sliced Document Number
Part No
Payment due date
Product name
Remarks (Invoice)
Source (Invoice)
Vendor ID
Payment provider location# Loc...
Amount payable (accounting curr...
Amount payable (accounting curr...
Line of the payable list# Amount p...
Invoice (Count)
Payment
Bank Account
Currency
Document Number
Document Status
Invoice ID
Payment Date
Payment Object
Payment Provider
Payment Sliced Invoice Number
Pages
Filters
Vendor ID
Marks
All
Bar
Color
Size
Label
Detail
Tooltip
Supplier receiving bank account
Measure Names
SUM(Total Amount)
SUM(Line of the payable list# Amo...
Columns
SUM(Total Amount)
SUM(Line of the paya..
Rows
Vendor ID
Amount paid in payment against amount paid in invoice
Line of the payable list# Amount payable (accounting currency)#
Vendor ID
0K
500K
1000K
1500K
2000K
2500K
3000K
3500K
4000K
4500K
F0017
S0040
F0090
F0040
F0086
F0154
NBSZ
F0170
F0019
F0108
J0060
F0044
F0026
J0058
F0004
S0080
F0070
F0046
F0118
J0028
F0003
F0072
F0056
S0016
J0043
F0096
J0019
F0071
35 nulls
0M
1M
2M
3M
4M
5M
6M
7M
8M
9M
Total Amount
Measure Na...
Line of th..
Total Amo..
Data Source
Payments to discontinued/deac...
Invoice paid vs Payment paid
Total value of overpayments
Disruptive Actors
Ghost Actors
Malicious Actors 3.1
Malicious Actors 3.2
499 marks
267 rows by 1 column
SUM(Line of the payable list# Amount payable (accounting currency)#): 31,266,728
Luke Tan

Standard

Show Me

Data | Analytics

Employee Master (Payroll Data)
income
Invoice (Accounts Payable Data)

Search

Tables

income.csv
- Date
- Description
- Division
- Employee Type
- Grade
- high std div employees
- Payment Sub Type
- Payment Type
- Relevant Income
- Amount
- Employee Master
- F1
- *income.csv (Count)*

payroll_employee.csv
- Adm Plan
- Bank Acct
- Bu Desc
- Bu Division
- Date Join
- Job Desc
- Employee Master (Payroll Employ...
- F1 (payroll employee.csv)
- *payroll_employee.csv (Count)*

- *Measure Names*
- divergence
- July
- *Measure Values*

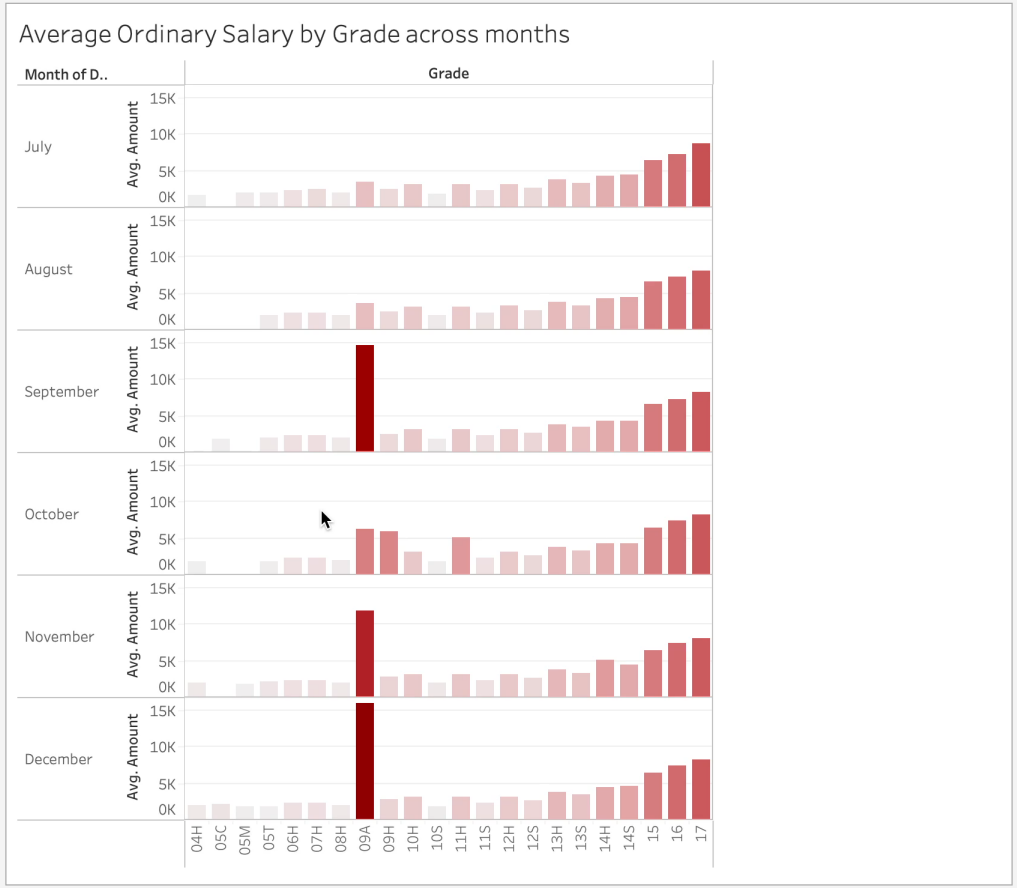
Pages

Filters
- Payment Sub Type
- AVG(Amount)

Marks
- Automatic
- Color
- Size
- Label
- Detail
- Tooltip
- AVG(Amount)

Columns: Grade

Rows: MONTH(Date) | AVG(Amount)

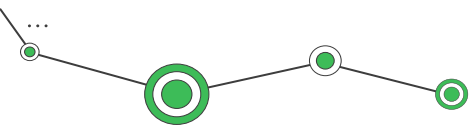


AVG(Amount)
1,719 — 15,975

Data Source | Disruptive 4A | Disruptive 4B | Disruptive 4C | Disrupted 5 | Ghost 3 | **Malicious 7** | Sheet 29 | Malicious -7.2 | Sheet 14 | Temp 5 | Malicious 8 | Malicious 9 | Malicious 10 | Malicious 10.2 | TEMP 1 | Temp 2

123 marks | 6 rows by 22 columns | SUM of AVG(Amount): 469,323

Vinay Krishnaa



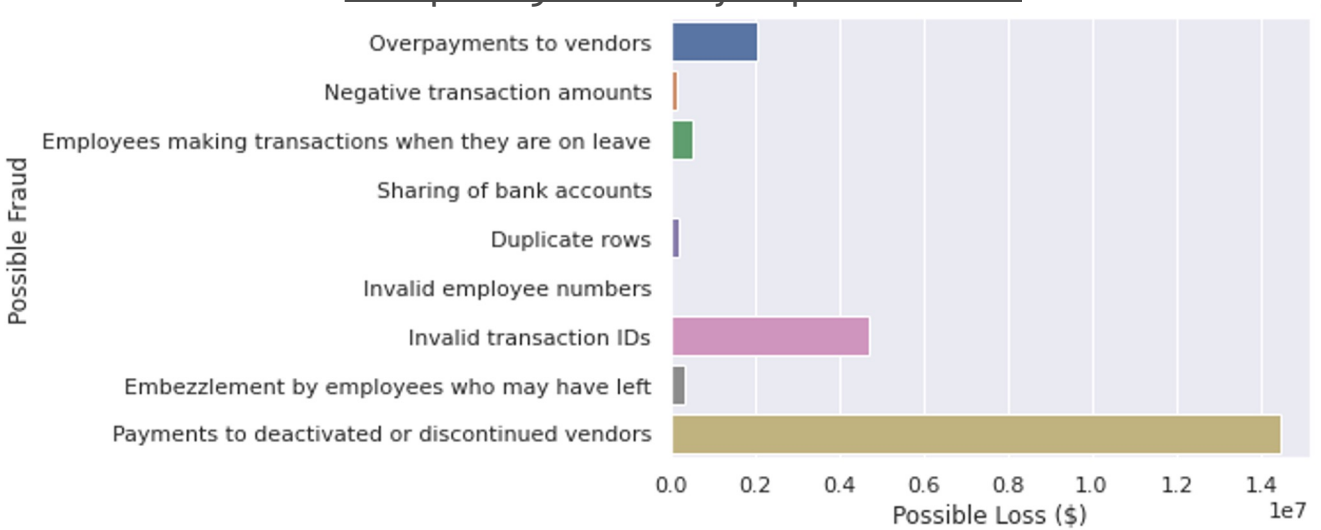
$22,494,831

Suspected Fraud Valuation

Outcomes

Which rules are the most effective?

Comparing monetary impact of rules



The rule which has the highest financial impact identified was the under payments to deactivated or discontinued vendors, with a total potential loss of **$14,445,195.10.**

Outcomes

Which Risk Profile is the Most Prolific?

Malicious Actors

- Highest number of possible rules
- Employees are exploiting difficult to notice loopholes
  - Crediting Lumbago for transactions even after leaving the company
  - Collaborating with “fraudulent authorisers”

There is a danger of system administrators - such as identified authorisers - for approving large numbers of fraudulent transactions.

Right Now: These rules flag out employees and those in positions of power so as to prevent such fraud

Future: We need to adopt Machine Learning models such as DBSCAN, such credit card transactions are flagged as fraud by their natural attributes

04

Recommendations

Recommendation

Handling Disruptive Actors

- Disruptive actors exist due to the lack of input control

- **Input control** can be implemented in the following ways:
  - User interface restricts type of input e.g. no alphabets in transaction ID input
  - User interface requires certain inputs to be keyed in for a transaction to be recorded
  - Normalised database implementation will restrict duplicate primary keys e.g. duplicate transaction IDs

Recommendation

Handling Ghost Actors

- **Strong internal controls**
  - Stringent access controls to authorise and verify employees
  - Multiple user access levels i.e. do not give access to employees that they do not need

  Aim: Prevents ghost actors from accessing system

- **Decentralised processes**
  - Actor making transaction should not be able to authorise his/her own transactions

  Aim: Prevents ghost actors from being able to make transactions from one point of access

- **White-listing**
  - List of pre-approved vendors should be updated regularly with update history well-documented

  Aim: Prevents money from flowing out to fake/outdated vendors

Recommendation

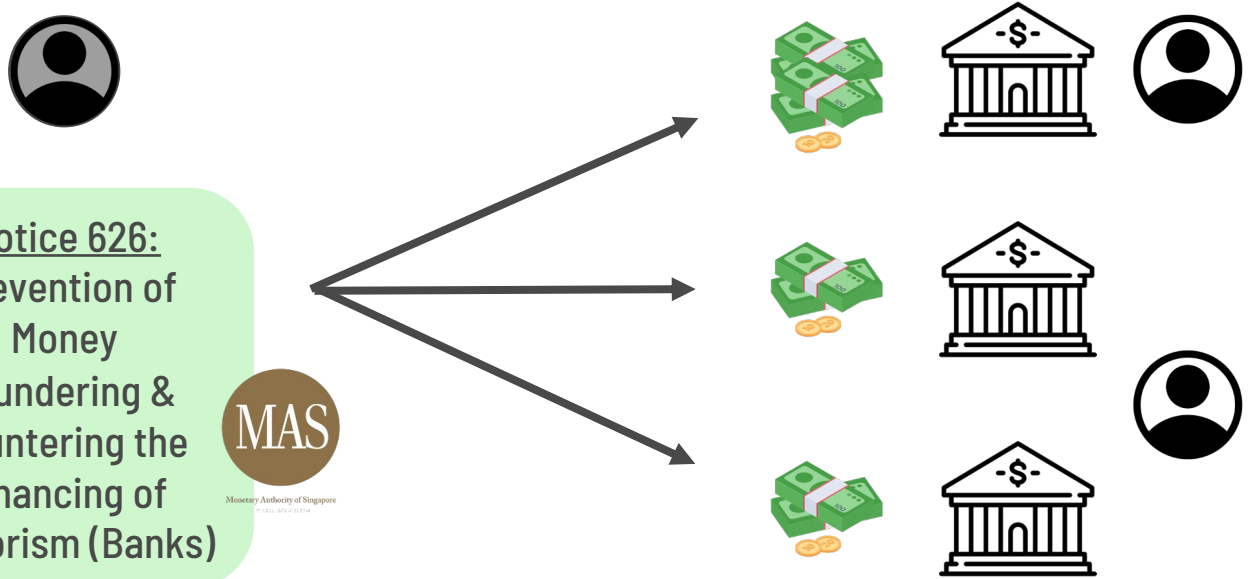
Handling Malicious Actors

- After sieving out disruptive actors and ghost actors, a more complex approach must be taken to detect malicious actors
- **Rules** developed in this case will be useful in flagging out future similar occurrences
- Increasing sophistication of malicious actors require an **adaptive & constantly evolving approach to fraud detection**
- **Regular data mining & analytics** is required to pick up on new trends and develop new rules
- A **strong whistleblower program** generates good starting points for data exploration and analytics
- **Established & extensive inter-bank communication**

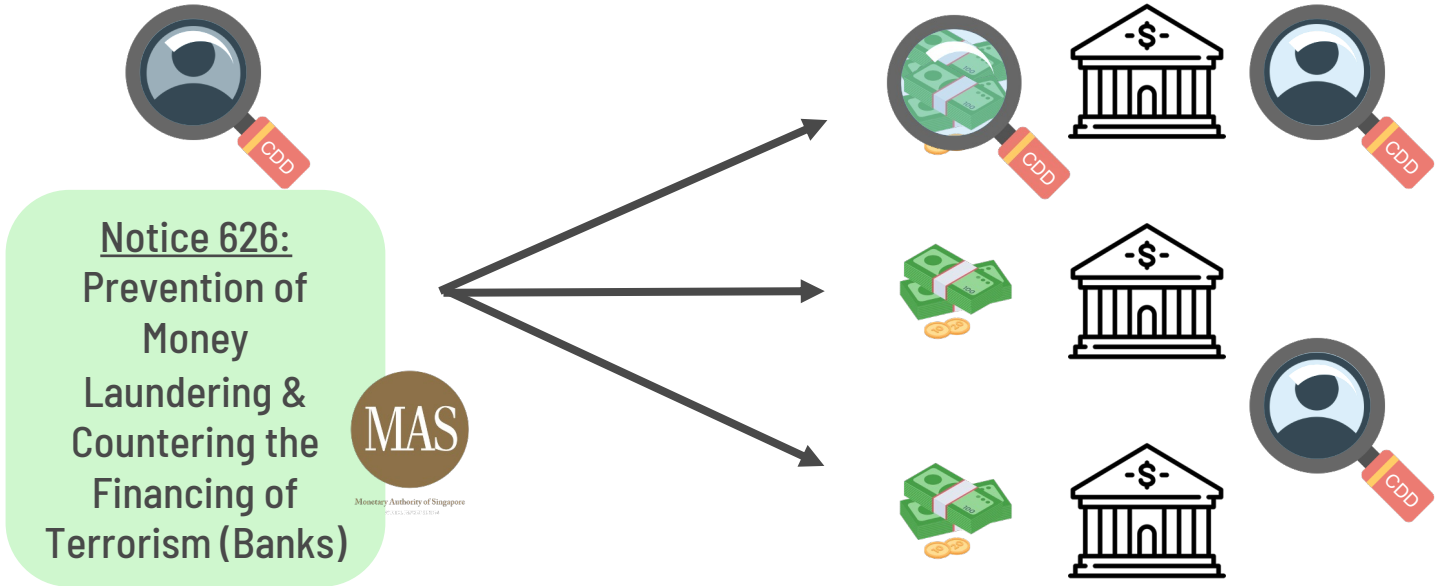
05
Laundering Detection

Structuring/Smurfing

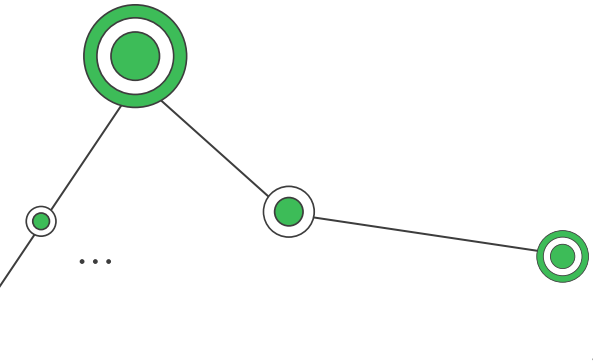
Structuring/Smurfing



Structuring/Smurfing

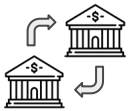


Scale of Detection



Intra-bank Smurfs

- Uses bank data
- Data readily available
- Single format & structure



Inter-bank Smurfs

- Aggregate multiple banks data
- Pending banks' agreement
- Pending architecture to support exchange of data
- Multiple formats & structures
- MAS initiative may alleviate issues

Detecting Smurfing

- **Customers with multiple accounts**
  - Perpetrator may have multiple accounts

  Requires: Accounts data + Transaction data

Rule-based

- **Shell customer**
  - Perpetrator may have multiple accounts under different aliases
  - E.g. check duplicate emergency contacts, NOK for different accounts

  Requires: Accounts data + Customer background check data

- **Linked customers**
  - Perpetrator may use relatives'/friends' accounts
  - E.g. check if family has high transaction activity

  Requires: Accounts data + Transaction data + Customer background check data

Detecting Smurfing

- **Grouping transactions**
  - Clustering based on transaction date, location, amount
  - Identify groups with large activity
  - Aims to reverse the smurfing process

  Requires: Accounts data + Transaction data + Customer background check data

Machine Learning

- **Generating new rules**
  - Accounts flagged out and verified as smurfing cases should be indicated in data
  - Enables supervised learning to identify patterns and form new rules
  - Reiterative process: flagged patterns can be used to train machine learning algorithms to detect future occurrences

  Requires: Accounts data + Transaction data + Customer background check data

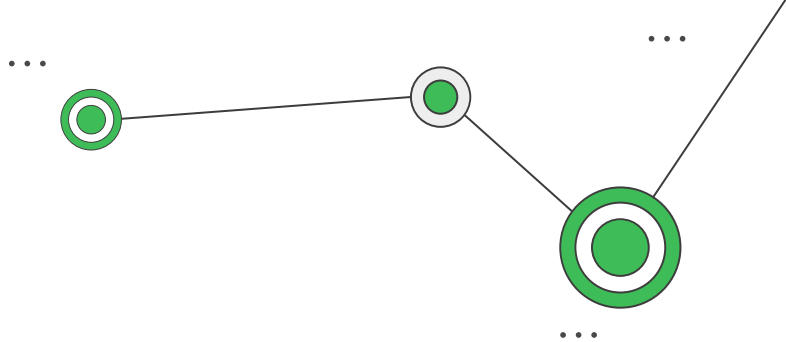
Conclusion

Combat Internal Fraud

Anti-Money Laundering System

***Grow* to be a champion of reliability and a *leader* in the market**

Deloitte.



Thank You

Investigating Fraud Utilising Advanced Analytical Techniques

NBS BAC Hackathon

VSLAM
Ananya Balehithlu | Bai Shun Yao | Max Tan Zheyuan
Tan Kit Hon, Luke | Vinay Krishnaa Vinod