Team FinHack

NBS BAC x Deloitte Business Analytics Hackathon 2022

NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE | Nanyang Business School

BAC NBS BUSINESS ANALYTICS CLUB

Deloitte.

Executive Summary

Macro Outlook

- Problem statement and Objectives
- Common fraud and Risk profiles
- Data used and limitations in analysis

Analytics and Insights

- Data mining applications used
- 9 Frauds detected
- Qualitative and quantitative analysis of frauds present
- Recommendations for financial loss minimisation and prevention

Regulations and Smurfs

- Money Laundering overview
- Local Regulatory legislations, historical, current and future strategies to counteract Money laundering
- Frame work, dataset required and methodologies required in Smurf detection

Sources: HSBC

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 (Overpayments)
4. False Billing
5. Duplicate Invoice Payment
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) • Overpayments	• Ghost Employee Fraud • Pay Rate Alteration Fraud • Unauthorized Employee Fraud • Fake Vendor Fraud	• Fictitious expenses • Miscategorization 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 & Payslip 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)
- Missing information in timeframe (November Month)

05

The Team’s Analytical tools

Analytical Tools

Data Mining and Discovery

Database storage

Data Visualisation and Storyboarding

06

Key Insights

Outcomes from Data Mining and Analysis

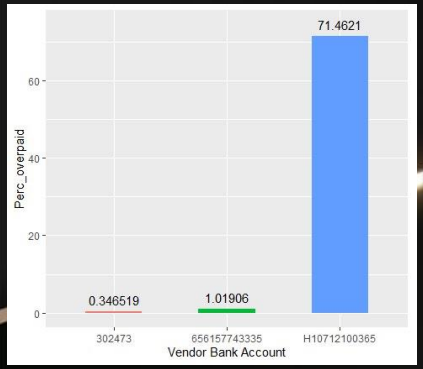
Accounts Payable Fraud

Billing Fraud

Accounts creation for invoices for goods and services that were either not delivered, or payment were taken for the individuals themselves. Anomalies in Billing Information, where the postal code and country reflected were different

- Cash outflows reached areas highly related to **Terrorism and Tax-Sensitive areas,** such as Middle East and Americas
- **Possible layering and placement of cash** in Anti-Money Laundering

Overpayments/ Overbilling



Bank account H10712100365 reflected the **highest percentage overpayment for settled transactions (71.46%)** and **highest transaction sum of $ 19,874,175.59.**

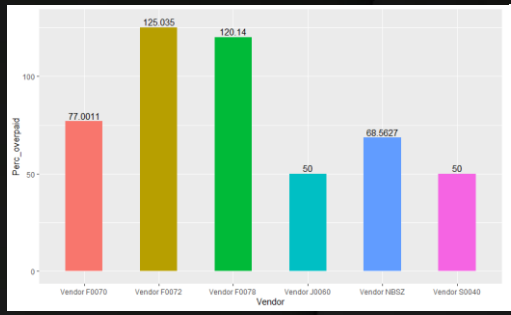
As these financial figures are obtained from the "Payments" Sheet, they will be deemed as **"Unrecoverable/Bad payments"**.

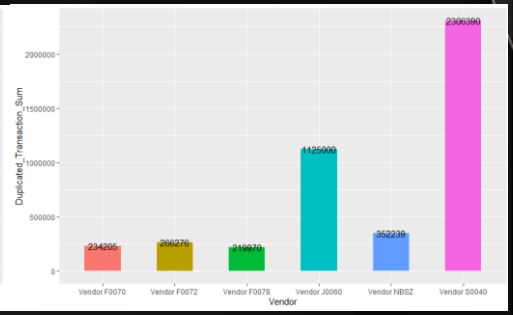
Duplicate Invoice Payments

Fictitious payments for items that were never purchased. or expenses that may be overstated to external vendors or external accounts. Data investigation made 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:

Sum of Duplicated Flow Transaction: SGD$ 6,079,815 (16.88% of total transactions)

Duplicated Accounts: 125 (> than 50% of Vendor accounts (53.65%))





Vendor S0040

- **Perc**
- **Dupl**

Vendor

- **SGD**
- **Employee's bank account was disguised as a vendor→ statistical correlation of Fraud.**

The accounting discrepancies and fictitious payments can signal possible money laundering within the bank involving external transaction accounts.

Credit Card Fraud

Duplicated Transactions

3524 instances of duplicated transactions amounting to $418,477.7 were found .The duplicated transactions involved multiple employees as well as vendors.

Assumption:

1) The team considers all duplicated transactions to be relevant in our fraud analysis
2) No data entry error that would cause duplicates

Instances

401 employees and 568 vendors involved in potential fraud.

103 instances of unsubmitted claims for credit card transactions were also present.

Personal Expenses

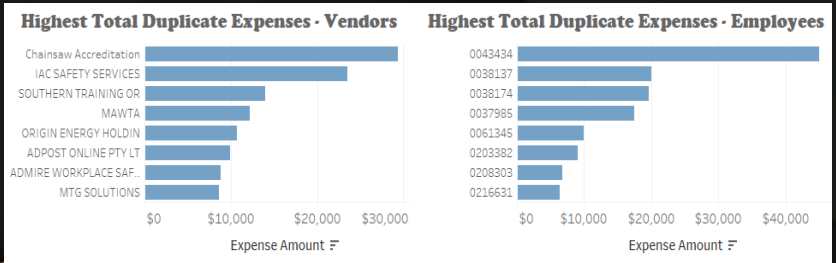
4,617 instances of credit card spending was done during leave days. The suspected personal expenses amount to $1,433,525.70 and involved multiple employees.

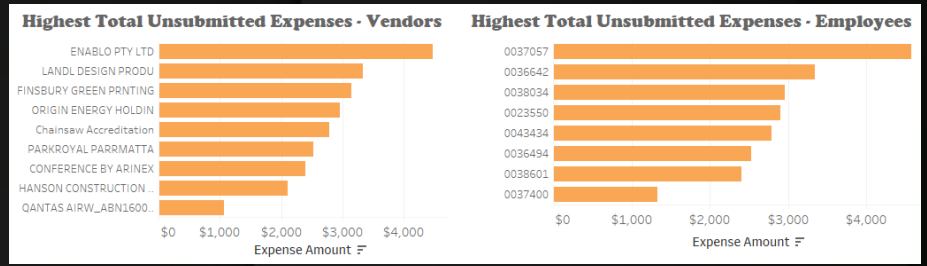
Assumption:

1) All employees are not allowed to use their corporate card while on leave
2) No permission granted for employees to override assumption 1
3) No Transaction Time – All spending on leave days are relevant

Instances

847 Employees





Payroll Fraud

Ghost Employee Fraud

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 & Mobile Number

	Employee_Master	Job_Desc	Mobile_Phone	Bank_Acct
1	0020186	Consultant	91030697	282-8803243
2	020186A	Managing Quantity Surveyor	91030697	282-8803243
3	0038776	Sr Project Manager	5555555555	5555555555
4	0454690	Building Rigger Labour	5555555555	5555555555

Instance 1 & 2

Assumption: Additional "A" was added to the end of the Employee ID which may signify a promotion/rotation

Implication: No salary pay-outs for these 2 instances

Instance 3 & 4

Both Employees IDs were paid during the same period

Assumption: One of them is Daily-Paid while another is Monthly-Paid. Employees with multiple roles/payment types should be paid to a single employee account for tax and accountability purposes.

Implications:

0038776 is the ghost employee: $121,208

0454690 is the ghost employee: $763.05

Conclusion: 038776 and 045490 is likely to be a ghost employee, further investigation required.

Home Phone

	Employee_Master	Home_Phone		Employee_Master	Home_Phone
1	0064264	23283560	9	0036630	26481189
2	0064265	23283560	10	0036675	26481189
3	0037981	23526426	11	0034964	26656742
4	0240513	23526426	12	0038562	26656742
5	0038389	23589927	13	0023791	35421285
6	0038412	23589927	14	0042009	35421285
7	0037057	26436624	15	0052468	35740403
8	0037935	26436624	16	0052992	35740403

Assumption:

1) Employees can have multiple bank accounts but only 1 home phone.
2) Home Phones entered are accurate and valid
3) Some Home Phone numbers including "8999" were excluded.

Conclusion: Inconclusive due to multiple instances, further investigation required.

Pay Rate Alteration/Advance Fraud

Pay Rate Alteration Fraud occurs when an employee with access to the payroll system alters the pay rate for some employees.

Advance Fraud occurs when an employee draws advances but attempts to avoid payment in several ways.

Assumption/Limitations:

1. In this case, since there are no hourly-paid employees, monthly changes is highlighted for further testing.
2. Advance is given due to the erratic nature of some monthly-paid employees. However, there are no information on advance given/paid outside of the period. Therefore, totality of changes is tested.

	Employee_ID	NetChange
1	0322446	62738.62
2	0475189	38685.27
3	0481748	33581.48
4	0474380	26805.60

Showing 1 to 5 of 1,358 entries, 2 total colum

Instances of Irregularities: 1358

Implication: Total $582,041, Single Employee Net Change up to $62,738.62 overdrawn.

Conclusion: While there are both overdrawn salaries and employees who had a net negative salary, the limitations of the dataset meant that it is hard to ascertain fraudulent pay rate or advances activity possible reasons may include bonuses, commissions, advances etc.

Payroll Fraud

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.

Assumption:

1) 38 Days used as a control as a buffer for last-month-salary – MOM requires employees to be paid within 7 days of end-of-period (MOM, n.d.) . Given that all employees have different contract end dates and the financial period is unknown to employees, 1 month is used as the buffer. Therefore, 31 Days + 7 Days = 38 Days.
2) Pensions are excluded as it can be paid beyond.

Employee_Master	Contractual	Contract_End	PayDate	Description	Amount
0037925	Yes	2020-12-16T00:00:00Z	2021-09-28T00:00:00Z	Salary/Wages	5346
0037925	Yes	2020-12-16T00:00:00Z	2021-09-28T00:00:00Z	Basic Allowance	1782
0037814	Yes	2021-06-30T00:00:00Z	2021-09-28T00:00:00Z	Salary/Wages	11232
0037814	Yes	2021-06-30T00:00:00Z	2021-09-28T00:00:00Z	Basic Allowance	3744
0052971	Yes	2021-09-11T00:00:00Z	2021-11-28T00:00:00Z	Salary/Wages	3850.56
0042908	Yes	2021-03-15T00:00:00Z	2021-12-28T00:00:00Z	Salary/Wages	3109.27

Instances

392 Employees were paid beyond 38 days of the end of their contract. Some as late as 9 months later as seen in instance 1

Implications:

Total = $10,222,561.24

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

False Vendor Fraud

False 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.

	Ven_ID	Name	Classification	Purchasing_department	Supplier_receiving_bank_account
1	F0086	Vendor F0086	Auxiliary Materials	General Purchase	3602004409006503217
2	NBSZ	Vendor NBSZ	Customer Class	Business Section	722466572132
3	S0068	Vendor S0068	Business Class	NA	722466572132
4	X0002	Vendor X0002	Business Class	NA	5555555555
5	X0003	Vendor X0003	Business Class	NA	5555555555
6	X0004	Vendor X0004	Business Class	NA	5555555555

Instance 1, 2 & 3

3 Instances of 2 Unique Vendor Bank Accounts are the same as 2 of the Employees

	Employee_Master	Bank_Acct
1	0290323	3602004409006503217
2	0321638	722466572132

Implications:

F0086 = $2,340,342
NBSZ = $1,744,018

Instance 4,5 & 6

Same bank account number as Ghost Employee Identified

Implication: No payments made, possible testing account or out of period.

Conclusion: 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.

Pension Allocation Fraud

Occurs when employees draw pension inaccurately or when they are not supposed to possibly instigated by external syndicates.

Assumption:

Negative Pension refers to pension members making contributions to their scheme

Allocation is made on calculation of Net Salary.

Filter

	Employee_ID	Date	MonthlyAmt	pension	givenpen	diff
1	0054281	2021-12-28	7667.3	383.36	383.37	0.01
2	0036873	2021-08-28	7887.3	394.36	394.37	0.01
3	0232117	2021-12-28	9057.7	452.88	452.89	0.01
4	0043345	2021-07-28	9805.3	490.26	490.27	0.01

wing 1 to 5 of 29 entries, 6 total columns

29 Instances of Rounding Error

Conclusion: No conclusive pension allocation fraud found

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 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.**

This is important as Money laundering can lead to negative effects such as reputation loss to the Bank.

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 to ensure that payments are legitimate
- 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 extraordinary (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.
- E.g. Payroll data → 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
- 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

Money Laundering Structuring/Smurfing

Money Laundering Process

Smurfing

- Deposits of ‘travellers’ cheques/bank drafts in small amounts to savings account
- Lack of KYC information on large cash inflow into bank accounts
- Cash inflows wired through false identities from other bank accounts

Layering

- Cash assets smuggled across borders (Large Cash outflow)
- Money exchangers used to layer the large financial assets

Integration

- Cash service used to ship banknotes back to public
- Wire transfers to public bank accounts
- Cash used to purchase material assets.

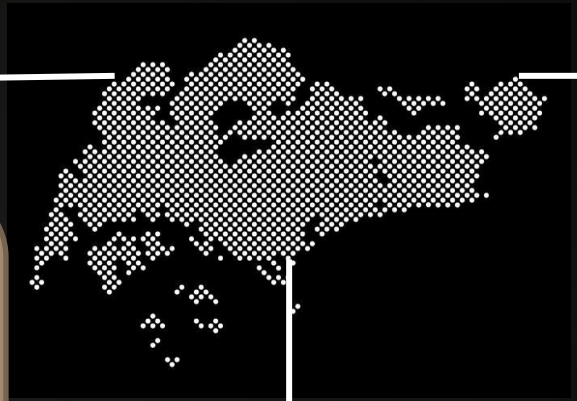
Local Regulatory Scene

MAS - NOTICE 626
Prevention of Money Laundering and Countering the Financing of Terrorism (MAS, 2021)

- ✓ Procedures & Requirements for Suspicious Transaction Reporting (Not exceeding 15 days of bank staff referral)
- ✓ Guidelines, Explanation and Illustrations of Money Laundering Cases and Suspicious Transactions
- ✓ 7 Measures to identify CDD & Give Authority to Banks to Perform CDD
- ✓ Requirement to include information of originator for cross-border transfers of more than S$1,500

Customer Due Diligence (CDD)
Anonymous or Fictitious Account
- No Bank Allowed to Open or Maintain Account

Customers with Reasonable Grounds for Suspicions based on historical activities
- Bank shall not establish business relations or undertake transactions and file Suspicious Transaction Report (STR)



Internal Controls and Audit department

→ **Singapore Police Force – Commercial Affairs Department:** Investigate Allegations of Money Laundering

→ **Suspicious Transaction Reporting Office:** Receives STR, Cash Movement Reports, Cash Transaction Reports

→ **MAS – Anti-Money Laundering Unit:** Approx. 30 Investigators

(Dow Jones, n.d.)

Moving Forward: Central data platform to counter Money Laundering

DBS · OCBC Bank · citibank · Standard Chartered · UOB · HSBC

- Collaborative Sharing of ML/TF Information and Cases (COSMIC) Platform (FY2023)
- MAS Partnership with 6 banks to securely share customer and transaction information where cross material risk thresholds exists
- Data and risk analytics to flag out suspicious individuals/transactions
- Regulatory and cybersecurity compliance to prevent data mistreatment and breach

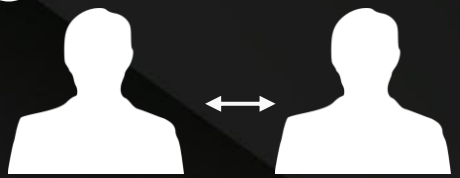
Payment Services Act (2022 Updates)
Licensing of Digital Payment Tokens and Services (Online Currencies) by streamlining payment gateways and services to reduce instance of utilizing online currencies for suspicious transactions

Detecting Smurfs/ Structuring

Network Analytics (Framework)

Steps:

1

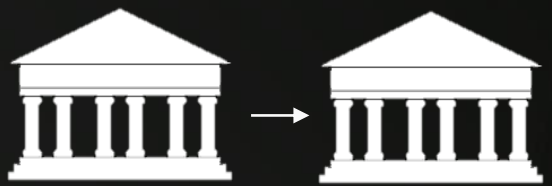


Identify Relationships

Define the relationships between each customer

1. Know-Your-Customer
2. Frequent Transfers
3. Payments

2



Build Connections

Visualising the flow of funds

1. Scrutinising transfers made by each account
2. Purpose of transfers

3

Discover Illicit / Suspicious Activities

Identify suspicious activities

1. Destination of funds
2. Discovering patterns

Detecting Smurfs/ Structuring

Dataset Required

1. Customer's Profile
   - KYC Purposes
   - Risk Profile
   - Customer Occupation, annual income
2. Customer's Close Contacts
   - Recipient of Transfers
   - Shared Accounts
3. Transfer/Payment Activity
   - Frequency
   - Date & Time
   - Purpose
4. Other Banking Activities
   - Foreign Currency Exchange
   - Withdrawals
   - Deposits

Methods

1. 80% Machine Learning, 20% Manual
   - Risk of False Positives
   - Consistent review required
2. Retrieve data in real-time
   - Real-time analysis of trends and patterns
   - Time series analysis
3. Grouping similar type of transactions
   - Spot anomaly between similar transactions
   - Identify trends within each account
4. Machine Learning Models
   - Association Rules
   - Neural Network/Deep Learning

QnA

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
- https://www.dowjones.com/professional/risk/glossary/anti-money-laundering/singapore/#:~:text=AML%20legislation%20in%20Singapore,money%20laundering%20and%20its%20criminalization.
- https://www.mas.gov.sg/-/media/MAS-Media-Library/regulation/notices/AMLD/notice-626/MAS-Notice-626---Banks.pdf

- https://www.mom.gov.sg/employment-practices/salary/paying-salary#:~:text=In%20accordance%20to%20the%20Employment,without%20notice%20and%20other%20situations.
- https://www.mas.gov.sg/news/media-releases/2021/mas-and-financial-industry-to-use-new-digital-platform-to-fight-money-laundering
- https://www.mha.gov.sg/mediaroom/speeches/association-of-banks-in-singapore-financial-crime-seminar-2021-deepening-partnerships-to-combat-financial-crime/
- https://shuftipro.com/blog/singapores-digital-payment-token-and-aml-regulations-2022-updates/#Singapores-AMLCFT-Laws-With-Respect-to-DPT-Services