

# Digital Financial Fraud May 2024

Viswanath Krishnamurthy  
Chief Risk Officer  
NPCI



# The Indian Landscape

## Population



**1.43 Billion**  
in 2023

India population is equivalent to  
**17.76%**  
of the total world population.

**35%** of the population is urban  
The median age in India is  
**28 years**

## Mobile Users



**1.01 Billion** Smart phones users in 2023

## Digital Population



Digital adoption is now being propelled by rural India  
**44%** more internet users from rural compared to urban sect

No of internet users stood at  
**692** million in the start of 2023

## Social Media Users



Social Network users were **467** Million in January 2023

Internet users set to reach  
**900** million by 2025

# Daily News that we see around us

A Nagpur man lost **Rs 9.70 lakh** to cyber fraudsters after falling victim to investment fraud (Source: Nagpur Today, 7 Mar'24)

Cybercriminals extorted **Rs 24.5 lakh** from a 58-year-old Reserve Bank of India employee by threatening her with arrest (Source: TOI, 12 May'24)

Retired IPS loses Rs **1.76 lakh** in cyber fraud in Mumbai, 1 arrested (Source: India Today, 16 Mar'24)

A retired Veteran duped of **Rs 2.28 Cr** on pretext of investment in share market after receiving dubious link on instant messaging app (Source: TOI, 19 Mar'24)



**60 Indians** Forced Into Cyber Fraud In Cambodia Rescued, To Return Home

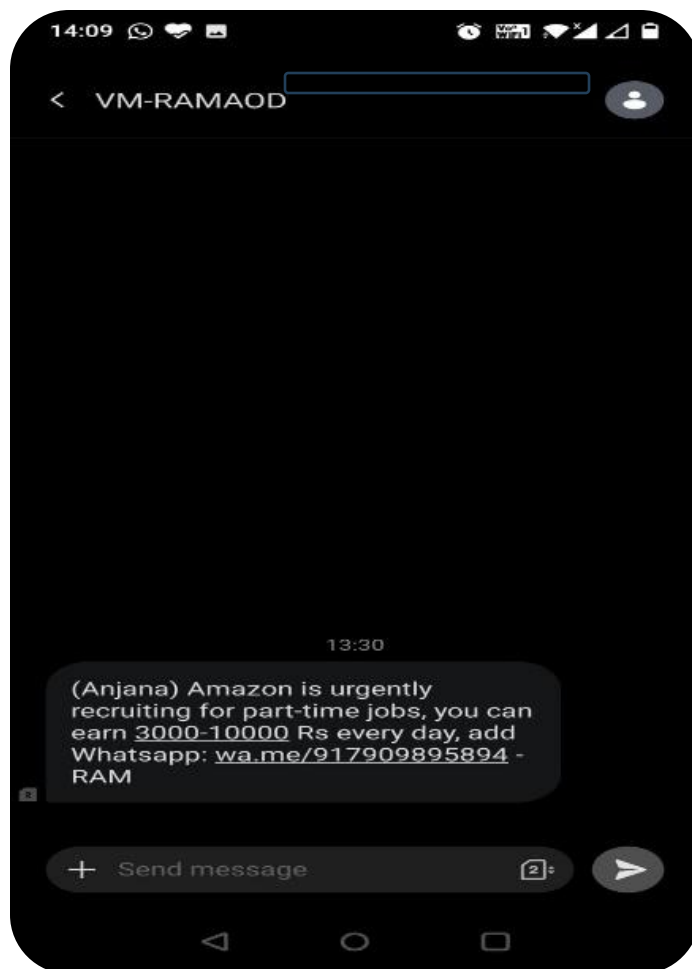


# **Social Engineering Frauds**

## **Investment Scam – Job/task Based**

# Investment scam – Job/Task based

User receives SMS with lucrative offer & Whatsapp link



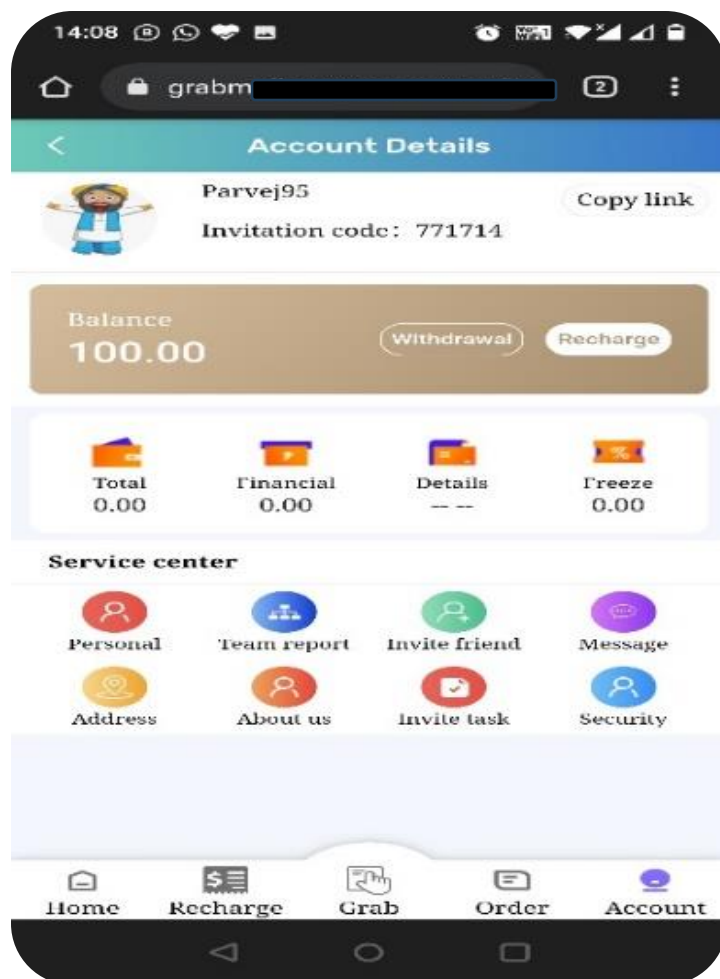
Link redirects user to scheme details and website link



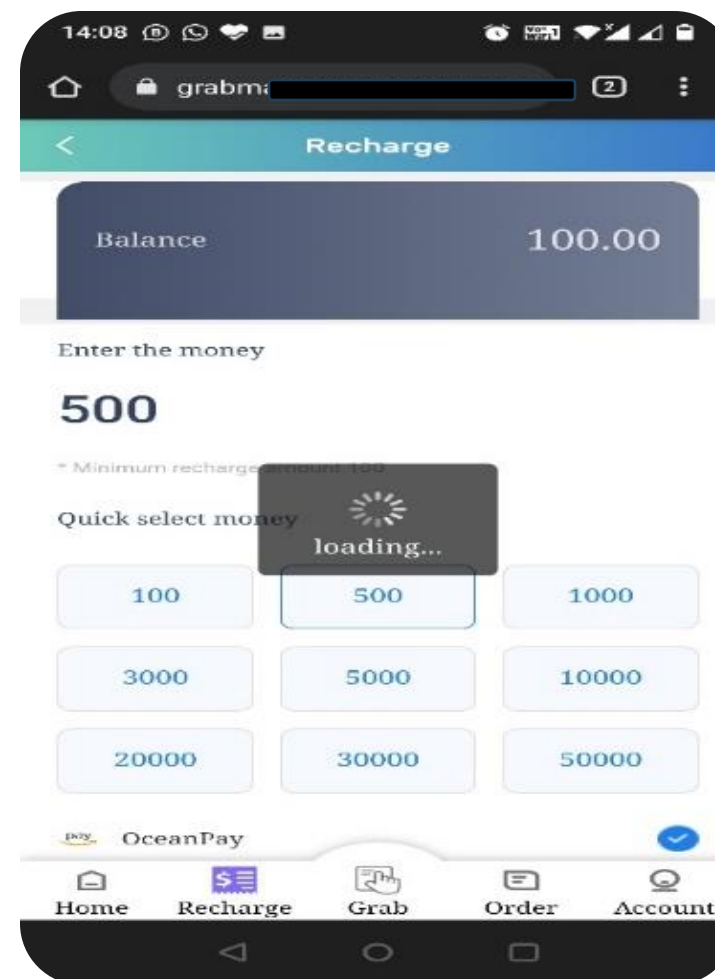


# Investment scam – Job/Task based

User registers himself on the website link/app

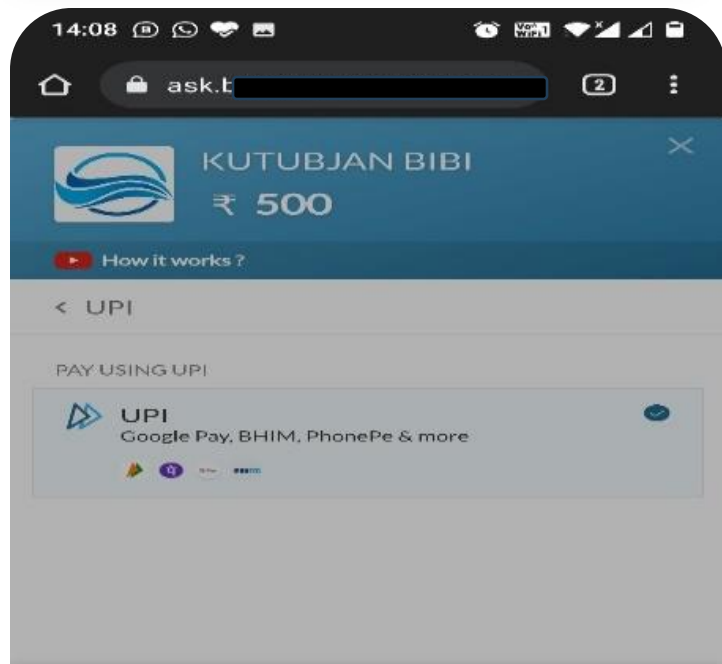


User is asked to invest/load funds



# Investment scam – Job/Task based

The payment options are available



Please wait until we confirm your payment



00:26



Sensitive customer info is sought

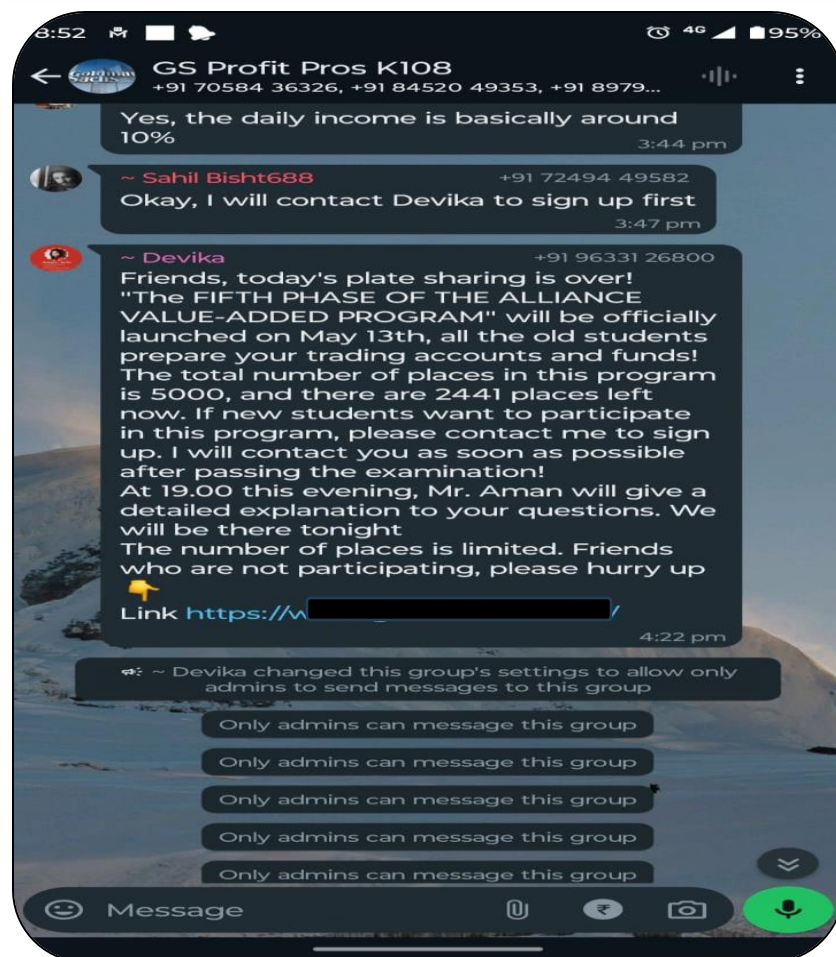


# **Social Engineering Frauds – Stock trading**



# Investment Scam - Stock trading

Victim, a Doctor by profession is added in an Instant Messaging group – ‘an alleged Stock Market Investing group’



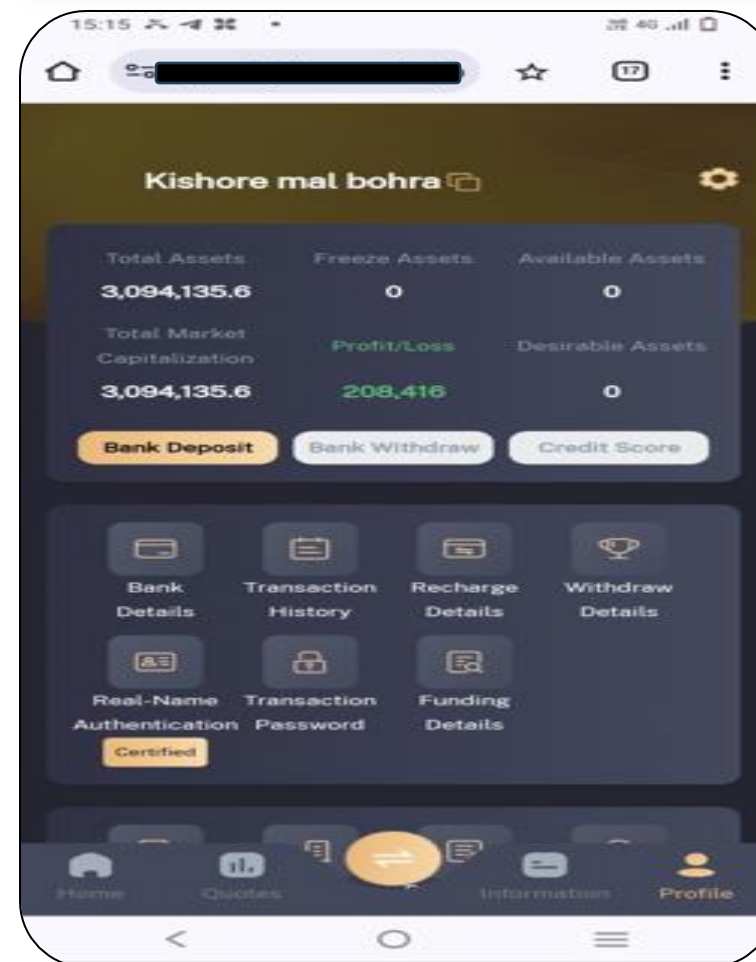
Alleged conversation in group builds trust & entices the Victim. to sign up into the link provided

# Investment Scam - Stock trading

Victim. is asked to make payment to different account numbers shared on instant messaging Apps



Investment portfolio screen shown to victim

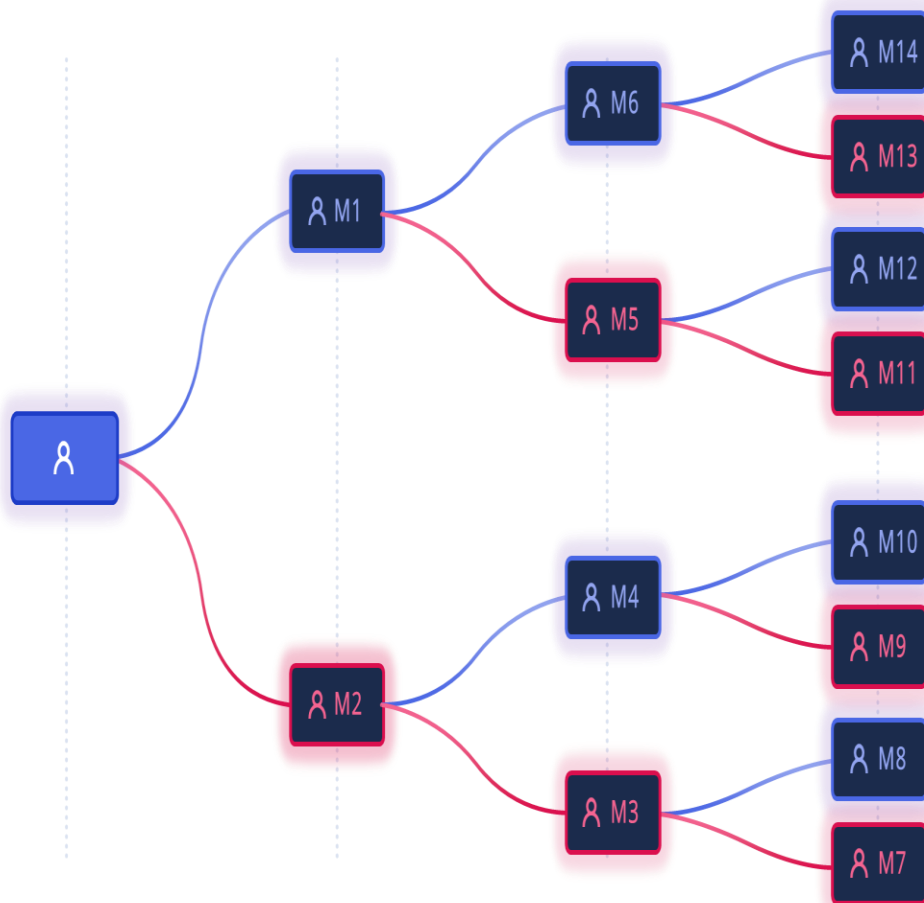


# Key Summary of Investment scam MO

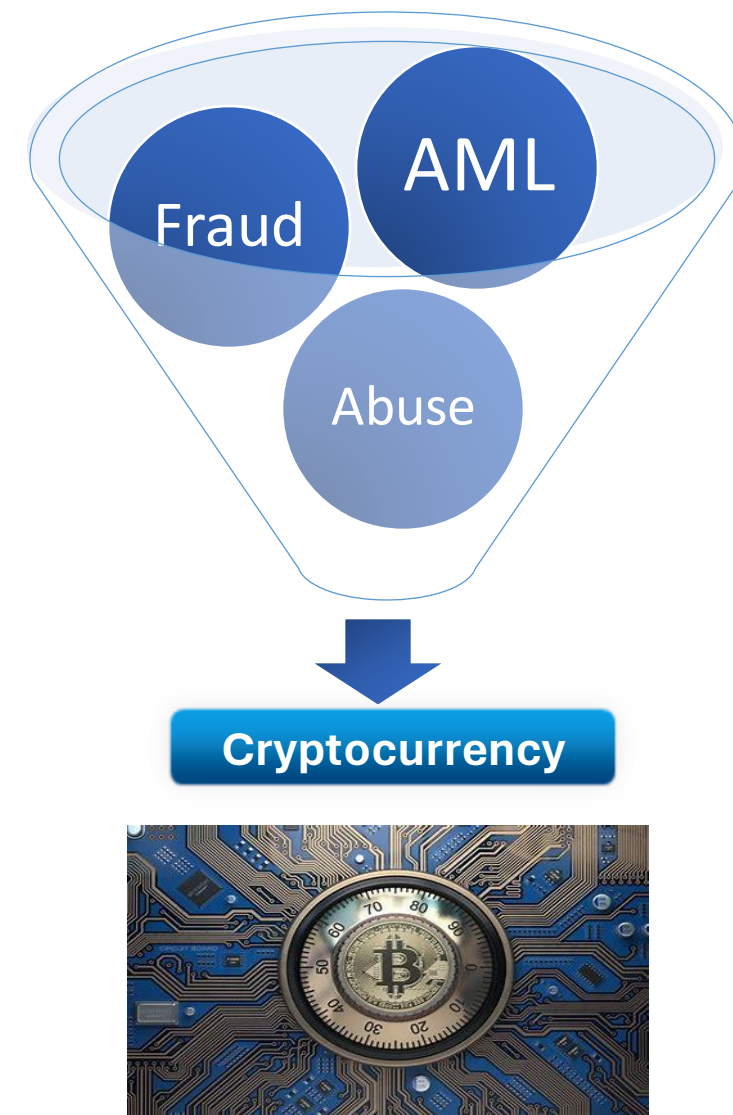


# Proceeds of crime exiting Financial ecosystem


Victim's fraud reported Bank Account



Fraudulent money exiting victim's bank account through numerous accounts in multiple hops







# **Social Engineering Frauds – Other Cyber Scams**



# Call from Fake LEAs (Digital Arrest)



More than **1,300 cases** of Digital Arrest Fraud Reported in Tamil Nadu in Just 5 months ( Source : The Hindu, 23 May 2024)

- Extorting money via Digital Payment channels
- India's cybercrime watchdog blocks over **1000 Skype IDs** used for online blackmailing ( The week, 14 May 2024)
- Govt working to Block Int'l Spoof Calls Duping Indians (ET, 24 May 2024)

- Victim receives call from cyber criminals posing as LEA officials
- Threats given on pretext of prohibited items with legal consequences
- Victim is summoned to come to a police station (Remote place)
- Victim is given an option for digital investigation ( Skype)
- Fraudster is disguised in LEA uniform over the video call to instil fear
- Victim is engaged for a few hours – '**Digital Arrest**'
- Ultimately, the victim is forced to make payment to forgo the matter

# SMS Forwarding Apps / APKs



Victim looks for courier helpline in online search engines & stumbles upon fraudster contact number

01



Fraudster shares phishing link and SMS forwarder APK (renamed as complaint tracker) & and Victim installs APK file their device which renders malware attack

02



Malicious application downloaded in victim's mobile device forwards OTPs and other sensitive information received on victim's device to pre-programmed numbers

03



Fraudster executes financial transactions using stolen credentials and OTPs sent to victim's RMN

04



# Fraudulent Digital Merchants

# Ineffective Merchant Onboarding practices



## Problem statement:



Customer complaining of not receiving goods/services



**Summary:** Such merchants approach gullible customers offering goods & services at discounted prices and vanish within a short time

- Fraudster has Current/ Savings account with the concerned Bank
- Fraudster onboards himself as a merchant **through Digital journey**
- Onboarding done basis old KYC **without “Merchant-Underwriting”**
- Default categorization as “online” leading to **bypass of controls**
- **High turnover** with negligible day end balances in such accounts
- **No monitoring** of transactions vis-à-vis customer’s profile
- No oversight on **complaints** coming against such merchants

# Challenges

01

**Customer doing transactions himself and ignoring verification call from Bank**

02

**Proceeds of financial crime is routed into multiple accounts in small tranches making it difficult to trace**

03

**Inadequate application of fraud tools using AI/ML to thwart such frauds**

04

**Inaction of mule accounts**

05

**Need for a comprehensive Negative Registry**

06

**Empowerment of Law Enforcement Agencies**



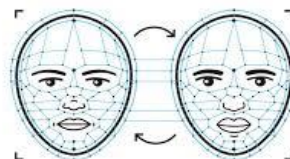


# Future Frauds



## Caller ID Spoofing Apps

- **Prevalence:** Numerous apps (Examples: Indycall, SpoofCard, Caller ID Faker)
- **Functionality:** Manipulate caller ID to appear legitimate
- **Impact:** Facilitates social engineering for payment info



## Deep Fakes

- **Definition:** AI-generated realistic videos/audios
- **Technologies:** GANs (Generative Adversarial Networks)
- **Applications in online payments:** Impersonation, Scams, Misinformation



## Future-Outlook

- **Increased Sophistication:** Advanced AI & spoofing techniques
- **Security Enhancements:** Multi-factor authentication and AI-based fraud detection
- **Public Awareness:** Education on recognizing/reporting frauds

# Singapore – Digital banking security measures – MAS & ABS

**Additional Authentication** for High-risk transactions

**Malware controls** implemented by major retail banks in Singapore.

**Default transaction limit** for online fraud transfers

**Money lock feature**  
(Money can only be transferred through Bank Branch visit)

Emergency self service **“kill switch”** for customers to suspend their accounts

Facilitate rapid **account freezing** and fund recovery operations



Scams in Singapore: 2023 – SGD **651.8 million** (46,563 cases) & 2022 – SGD **660.7 million** (31,728 cases)



# System Glitches

# System glitch led cyber criminals to money heist



## Problem statement:

Customer realises a glitch in Bank's system and exploits it to make money

- Customer (CM) of Bank A initiates online transfer of money to CM of Bank B
- Bank B credits its CM based on transaction received from Bank A
- Bank A receives a decline response from Bank B erroneously
- As a result, Bank A returns the funds to its CM
- Multiple CM of Bank A realizes the lapse to carry out transactions worth Cr.
- Bank B is now out of funds since Bank A does not pay any money to Bank B
- Bank B failed to realize sudden spike in declines
- Bank B failed to conduct reconciliation of transactions
- Cause - Changes to be done in UAT were mistakenly done in production
- Vendor staff was given access to production system
- Same 'login credentials' were used by multiple vendor staff



# Thank You