Public Policy Aspects of Tackling Payment Fraud

Nandkumar Saravade

An Old Story

- Retired as DG, EME, in 1986
- Now 93 years old, has two accounts: pension & checking
- Never used mobile/internet banking
- ‘Bank representative’ visited on 27 November and installed apps
- Multiple transfers, totalling ₹ 19 lakh

Lt Gen (Retd) Sushil Kumar, PVSM

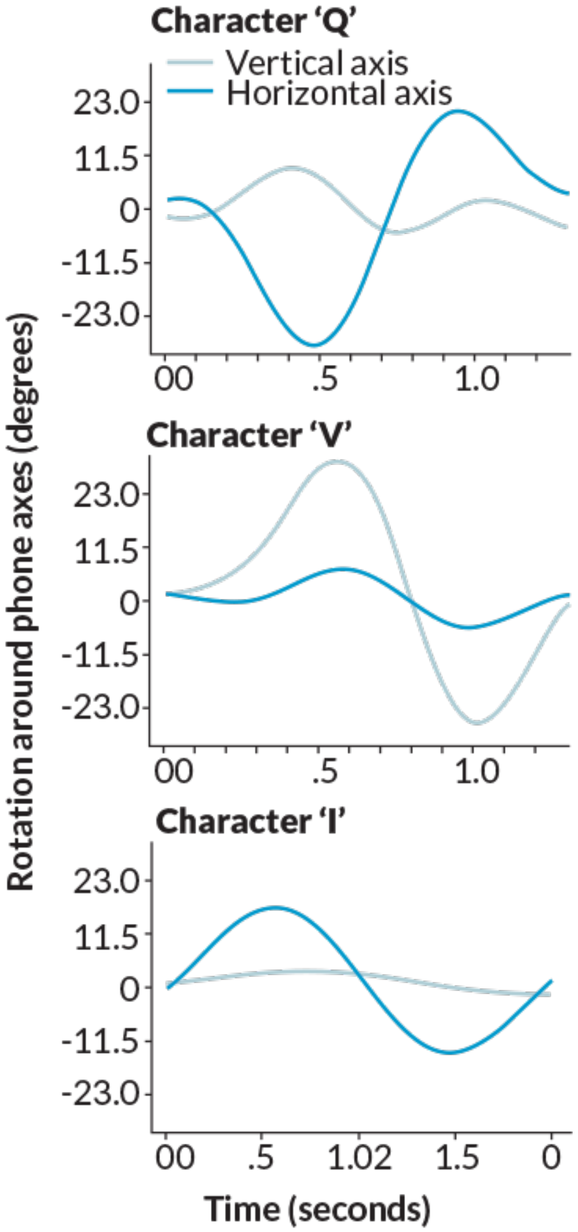
Some Follow Up Questions

- Was there a **data leak** in the bank? Has it logged into its systems who viewed Gen Kumar's account details in the last few weeks?
- How does the bank protect **senior citizens**? Why did it not have in place **velocity-checks** to detect that the large balance in the pension account was getting depleted rapidly?
- Will this case be classified as '**customer negligence**' under the RBI circular on liability for cyber frauds? Does a normal citizen have any chance against the wily and organised cyber criminals, who hone their skills every day?
- Given the fact that banks lost only **₹ 319 crore in cyber frauds in last three years, as compared to ₹3,83,504 crore stolen by large borrowers in loan frauds**, should they not treat cyber victims better without making them run from pillar to post, or worse, denying them any relief?
- Is the effectiveness of RBI circular on cyber fraud liability being checked, and different banks' practices compared? What is the efficacy of Banking Ombudsman system in giving relief in such cases? Is there an **audit framework** for checking a bank's Fraud Management including prevention, detection and response?
- Do the **police have adequate capacity** to triage and take up large value cases on priority? Do they/the concerned bank have an effective way of **freezing funds** in beneficiary accounts, before they are withdrawn in cash through ATMs?

What chance do you have of protecting your data?

I spy with…

- **Fingerprint**/TouchID: Scans the user's fingerprint
- **Proximity**: Measures the distance of other objects from the phone's touch screen
- **Light**: Gauges the light level in the phone's environment
- **Barometer**: Measures ambient pressure around the phone
- **Accelerometer**: Measures acceleration of the device's movement or vibration
- **Magnetism**: Reports the magnetic field intensity around the phone
- **Gravity**: Measures the force of gravity
- **Gyroscope**: Evaluates degree and direction of a phone's rotation. Can detect keystrokes based on unique signatures for each alphabet [https://www.sciencenews.org/article/smartphones-data-collection-security-privacy] With such ability, malicious apps can steal user data, including passwords with 99% accuracy, as the adjoining graphic illustrates



Data Protection, Privacy and Big Data

- Data Protection: The rules and safeguards applying under various laws and regulations to personal data about individuals that organizations collect, store, use and disclose.
  - Importantly, data protection is different from data security, since it extends beyond securing information to devising and implementing policies for its fair use.
- Privacy: Traditionally defined as "**a right to be let alone**" (Harvard Law Review, 1890). Now transformed by massive, technology-driven datafication and **spatial/temporal aggregation**
- Big Data/AI issues: **Volume, Velocity and Variety**, supplemented with **Value, Veracity, Visibility and Visualisation**
  - Increased difficulty in
    - protecting or **screening** out personal data
    - **de-identifying data** within datasets
    - increased possibilities for **re-identifying** individuals based on comparing data across data sets.
  - The need for large amounts of data during development as "training data" creates consent concerns

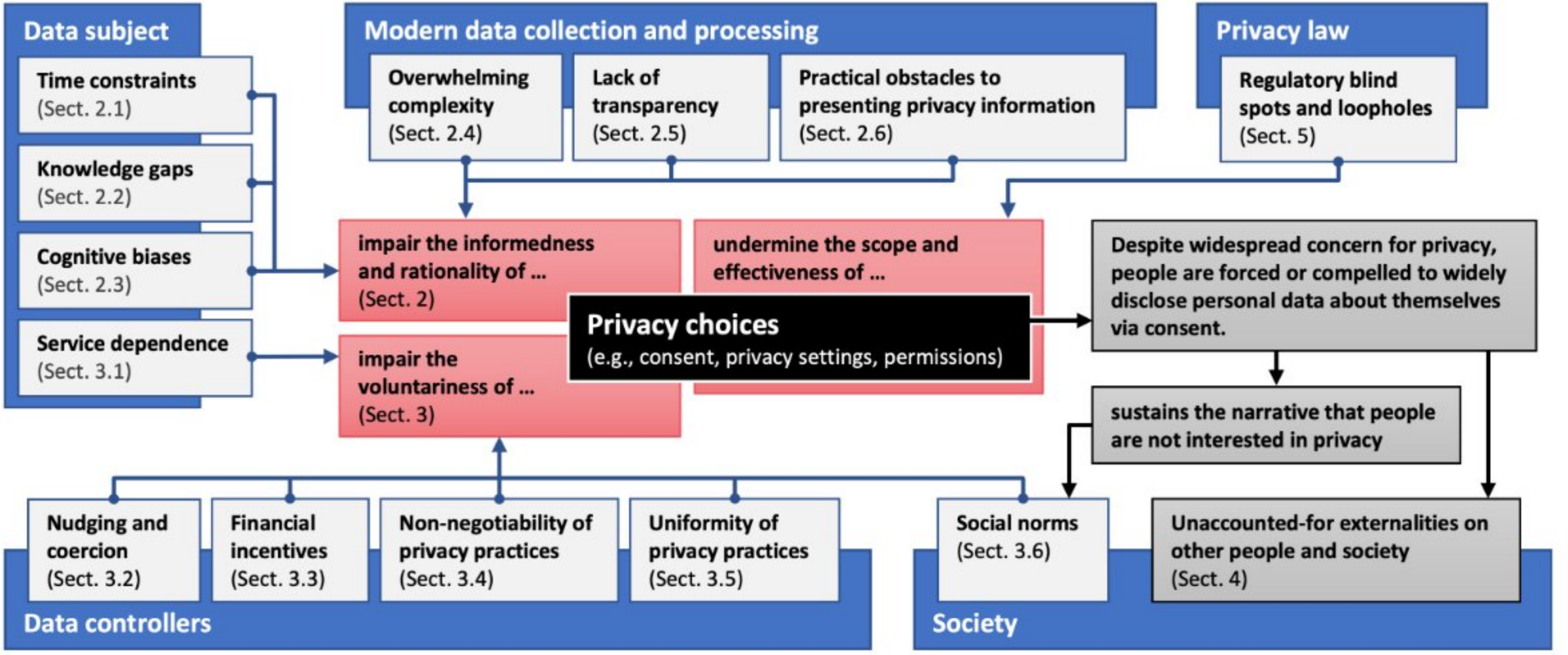


Figure 1. Overview of obstacles to the meaningful exercise of privacy self-management Source: https://ssrn.com/abstract=3881776

Background theory

Sizing up the problem

- Payment growth is spectacular, but there is much **headroom** left
- Malicious activity is automated and goes up relentlessly
  - As per CERT-In, a total of 14,02,809 and 13,91,457 cybersecurity incidents were reported for the years 2021 and 2022 respectively. The numbers will go up further with mandatory reporting now in place.
- Law enforcement **bandwidth** is limited and can be diverted to high-priority areas like public order maintenance, elections and such
  - Indian Cyber Crime Coordination Center (I4C) operates seven platforms like reporting portal, a cyber threat analytical unit, a cybercrime investigation task force, and a research centre. So far, more than **20 lakh cybercrime complaints** have been registered on the portal, with **40,000 converted into FIRs**.
  - Total cognizable crime during 2021 was 60.93 lakh, of which 1.74 lakh was economic crime and 0.53 lakh was cybercrime, compared to 7.62 lakh cases of property crime (thefts etc.)
- Bottom Line: **Prevention** needs to take precedence in design and operation of payment systems

Bank Fraud Trends

Table VI.2: Fraud Cases - Bank Group-wise

(Amount in ₹ crore)

Bank Group/Institution	2018-19		2019-20		2020-21	
	Number of Frauds	Amount Involved	Number of Frauds	Amount Involved	Number of Frauds	Amount Involved
1	2	3	4	5	6	7
Public Sector Banks	3,704 *(54.5)*	64,207 *(89.8)*	4,410 *(50.7)*	1,48,224 *(79.9)*	2,903 *(39.4)*	81,901 *(59.2)*
Private Sector Banks	2,149 *(31.6)*	5,809 *(8.1)*	3,065 *(35.2)*	34,211 *(18.4)*	3,710 *(50.4)*	46,335 *(33.5)*
Foreign Banks	762 *(11.2)*	955 *(1.3)*	1026 *(11.8)*	972 *(0.5)*	521 *(7.1)*	3,315 *(2.4)*
Financial Institutions	28 *(0.4)*	553 *(0.8)*	15 *(0.2)*	2,048 *(1.1)*	25 *(0.3)*	6,839 *(4.9)*
Small Finance Banks	115 *(1.7)*	8 *(0.0)*	147 *(1.7)*	11 *(0.0)*	114 *(1.6)*	30 *(0.0)*
Payments Banks	39 *(0.6)*	2 *(0.0)*	38 *(0.4)*	2 *(0.0)*	88 *(1.2)*	2 *(0.0)*
Local Area Banks	1 *(0.0)*	0.02 *(0.0)*	2 *(0.0)*	0.43 *(0.0)*	2 *(0.0)*	0 *(0.0)*
Total	**6,798** ***(100.0)***	71,534 ***(100.0)***	**8,703** ***(100.0)***	1,85,468 ***(100.0)***	**7,363** ***(100.0)***	138,422 ***(100.0)***

Areas of Concern

Table VI.3: Fraud Cases – Area of Operations

(Amount in ₹ crore)

Area of Operation	2018-19		2019-20		2020-21	
	Number of Frauds	Amount Involved	Number of Frauds	Amount Involved	Number of Frauds	Amount Involved
1	2	3	4	5	6	7
Advances	3,603 *(53.0)*	64,539 *(90.2)*	4,608 *(52.9)*	1,81,942 *(98.1)*	3,501 *(47.5)*	1,37,023 *(99.0)*
Off-balance Sheet	33 *(0.5)*	5538 *(7.7)*	34 *(0.4)*	2445 *(1.3)*	23 *(0.3)*	535 *(0.4)*
Foreign Exchange Transactions	13 *(0.2)*	695 *(1.0)*	8 *(0.1)*	54 *(0.0)*	4 *(0.1)*	129 *(0.1)*
Card/Internet	1,866 *(27.5)*	71 *(0.1)*	2,677 *(30.8)*	129 *(0.1)*	2,545 *(34.6)*	119 *(0.1)*
Deposits	593 *(8.7)*	148 *(0.2)*	530 *(6.1)*	616 *(0.3)*	504 *(6.8)*	434 *(0.3)*
Inter-Branch Accounts	3 *(0.0)*	0 *(0.0)*	2 *(0.0)*	0 *(0.0)*	2 *(0.0)*	0 *(0.0)*
Cash	274 *(4.0)*	56 *(0.1)*	371 *(4.3)*	63 *(0.0)*	329 *(4.5)*	39 *(0.0)*
Cheques/Demand Drafts, *etc.*	189 *(2.8)*	34 *(0.1)*	201 *(2.3)*	39 *(0.0)*	163 *(2.2)*	85 *(0.1)*
Clearing Accounts, *etc.*	24 *(0.4)*	209 *(0.3)*	22 *(0.2)*	7 *(0.0)*	14 *(0.2)*	4 *(0.0)*
Others	200 *(2.9)*	244 *(0.3)*	250 *(2.9)*	173 *(0.1)*	278 *(3.8)*	54 *(0.0)*
Total	**6,798** ***(100.0)***	**71,534** ***(100.0)***	**8,703** ***(100.0)***	**1,85,468** ***(100.0)***	**7,363** ***(100.0)***	**1,38,422** ***(100.0)***

Some open questions

- How big is the fraud problem?
  - ACFE estimates: $4.5 trillion!
  - RBI annual report (last three years, only for India)
    - Loan frauds: **$51.55 billion**
    - Payment frauds: **$42.88 million**
  - Global card fraud: $28.65 billion (2019), projected to go up to $38.5 billion in 2027 (6.1 basis points)
- How much research/theory in fraud management?
- How will technology change the nature of fraud?

What is special about cyber risk?

- There are adversaries on the other side
  - Operating in a developed marketplace/innovative/with global allies/tolerated or nurtured by nation states
- Increasing attack frequency + diminishing technology cost
- Adaptive and dynamic, complicating risk assessment
- Attribution challenges, amid low cross-border collaboration
- The true aggregation of risks goes well beyond the internal monitoring and risk management capacities of individual institutions
- 90% of the total costs are attributable to indirect factors/true cost of cyber-attacks manifests only over several years

A rudimentary issue: Fraud definition

- ‘A deliberate act of omission or commission by any person, carried out in the course of a banking transaction or in the books of accounts maintained manually or under computer system in banks, resulting into wrongful gain to any person for a temporary period or otherwise, with or without any monetary loss to the bank’. [From Gopalakrishna Working Group report]
- Two banks; similar card base but different criteria
- It suits everyone to not define fraud and undermeasure it.

Stakeholder Mapping

FinTech / Banks

- Have first line data
- Will not share except when forced by LEA
- Lack taxonomical awareness
- Incur cost on interacting with LEA, compliances, Fraud/Risk Teams

[Source: DeepStrat presentation]

Law Enforcement

- Have street presence and law enforcing power
- No understanding of the problem at a macro level.
- Very operational and tactical.
- See only a small portion of the problem.
- Hence ask for way too much information

Regulators

- Rule making Powers
- High level understanding
- Fiat rule making (e.g. Sharing Mandates)

Others

- Government (MoF/MeitY/states)
- Telecom/E-mail service providers
- Networks (NPCI/visa/ MasterCard)
- Merchants: E-com + B&M
- Consumers

Towards a taxonomy of payment frauds

- **Objects** – ID Document, Mobile#, UPI IDs, Bank Accounts, Domains, Email IDs, Links (PG Links), Wallets, Actors, Gangs etc.
- **Relationships** – Procured, Used, Opened, Transferred, Took Loan etc.
- Constraints – Modus Operandi are largely similar (Reference: Deepstrat Study).
- Need to express all this in a **Structured Format and Exchange** with all participants.
- Participants are both consumers and providers -> Key Principle of **Collective Defense** = All for One, One for All.

[Source: DeepStrat presentation]

Whose responsibility is it?

RBI Kehta Hai…

- Customer Protection - Limiting Liability of Customers in Unauthorised Electronic Banking Transactions (6 July, 2017)
- 24x7 access through multiple **channels** (at a minimum, via website, phone banking, SMS, e-mail, IVR, a dedicated toll-free helpline, reporting to home branch, etc.)
- **Negligence** by a customer, e.g. sharing of the payment credentials: Customer to bear the entire loss until he reports the unauthorised transaction to the bank.
- Third party **breaches**: zero liability for reporting within three working days
- Shadow reversal within 10 working days from the date of such notification by the customer.
- **Burden of proving customer liability** in case of unauthorised electronic banking transactions shall lie on the bank.

[https://www.rbi.org.in/scripts/notificationuser.aspx?id=11040]

Voices from elsewhere

- Singapore
  - Workers' Party chairman Sylvia Lim: "Banks should take on an outsized role in preventing them. Banks are able to **monitor** transactions, **block** suspicious payment flows and keep abreast of the latest **technological developments**. Such endeavours are **beyond the remit** of most bank customers."
  - Ms Lim also suggested reintroducing **physical tokens** as the default measure for two-factor authentication (2FA). With most banks offering only digital tokens or SMS verification for 2FA, Ms Lim said the mobile phone becomes a **single source of vulnerability**. If the phone is infected with malware, this 2FA would be ineffective.

https://www.straitstimes.com/singapore/politics/banks-should-reimburse-scam-victims-suggests-wp-s-sylvia-lim-govt-says-it-may-lead-to-complacency

Singapore recipe for phishing frauds

How will the SRF be implemented?

A “waterfall” implementation approach

FI, with primary role as fund custodian, assesses whether it has fulfilled its SRF duties. If the FI has breached any SRF duties (e.g. duty to provide outgoing transaction notification(s)), it is expected to payout.

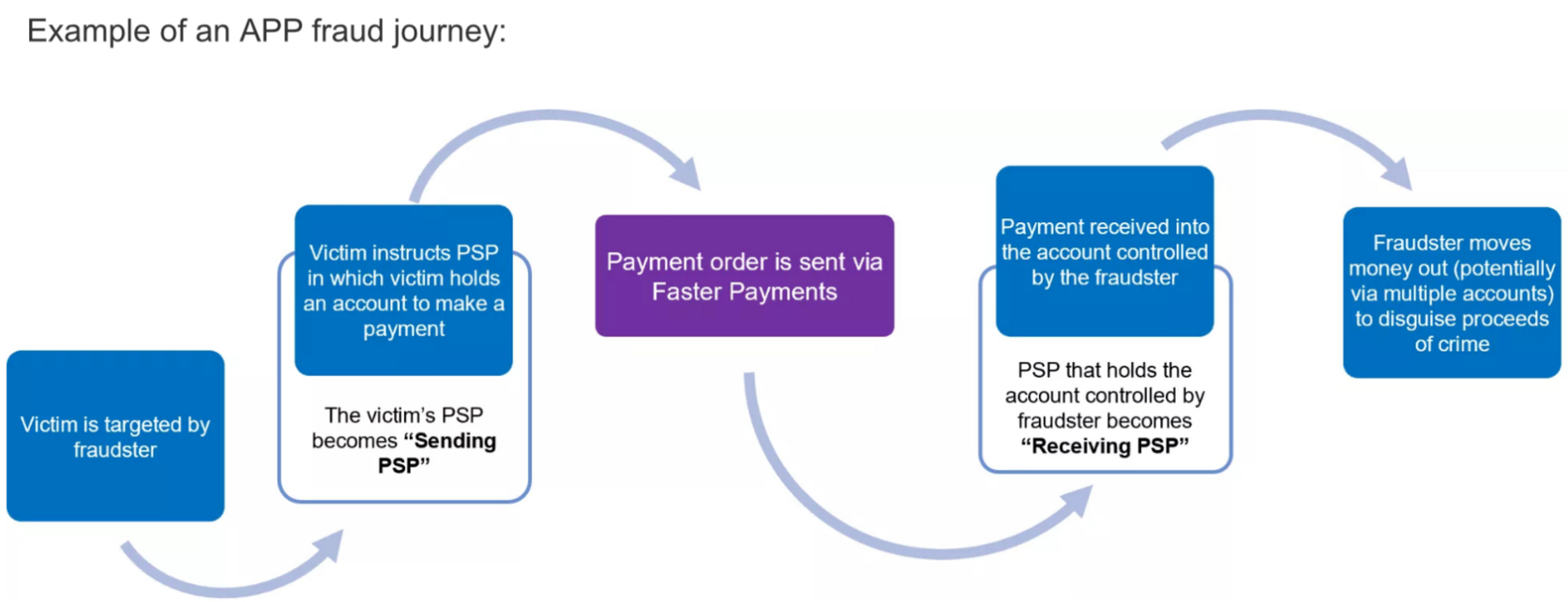
If the FI fulfilled all its duties

Telco, with secondary role as supporting infrastructure player, assesses whether it has fulfilled its SRF duties. If the Telco has breached any SRF duties (e.g., duty to implement anti-scam filter over all SMS), it is expected to payout.

If the Telco fulfilled all its duties

No payouts to Consumer under the SRF if both FI and Telco fulfilled all their duties.

UK's APP Fraud Initiative



- What is Authorised Push Payment fraud?
  - Scenario 1: Wrong Recipient
  - Scenario 2: Wrong Purpose
  - £459.7million losses in 2023

https://kpmg.com/uk/en/blogs/home/posts/2023/06/app-fraud-publication.html

What is the standard of care expected?

- **A requirement to have regard to warnings**: Consumers should have regard to specific, directed warnings raised by their PSP. These must occur before an authorised push payment is executed and make clear that the intended recipient of the payment is likely to be a fraudster.

- **A prompt reporting requirement**: Consumers who learn or suspect that they have fallen victim to an APP scam should report the matter promptly to their PSP. In any event, they should report it no more than 13 months after the last relevant fraudulent payment was authorised.

- **An information sharing requirement**: Consumers should respond to any reasonable and proportionate requests for information made by their PSP. This is to help them assess a reimbursement claim and whether the consumer is vulnerable, taking account of our ‘stop the clock’ rules.

What will the PSPs do?

- Specific warnings for the customer (to be raised by their PSP) would occur **before an authorised push payment is executed**, and where those warnings show that the intended **recipient of the payment is likely to be a fraudster**.
- The warnings should be **consumer, scam and transaction-specific**.
- The degree of **negligence** that may be deemed to rest with the consumer should consider, among other factors:
  - the nature of the **warnings** provided by their PSP
  - the **complexity** of the scam to which the consumer has been subject
  - any claims **history** from the consumer suggesting a propensity to fall for similar types of scams
  - whether the PSP can reasonably be expected to have paused or otherwise prevented an authorised push payment from being executed

https://www.psr.org.uk/our-work/app-scams/

How does the reimbursement work?

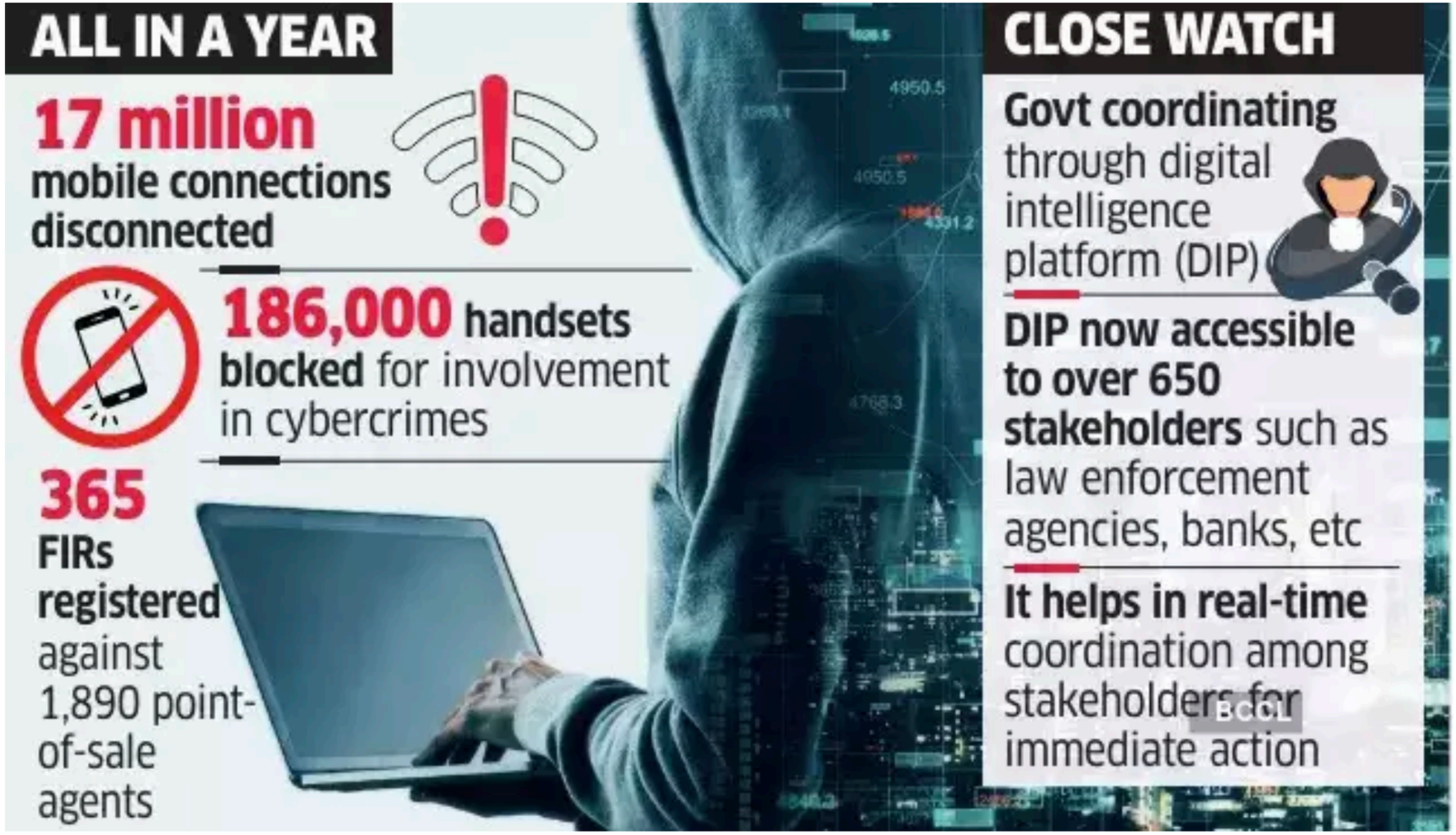
- Sending PSPs will have to reimburse the victim of an APP fraud, within **five days**.
- Sending PSPs will then seek contribution for the costs of reimbursement from the Receiving PSP.
- The costs of reimbursement will then be allocated equally between the Sending PSP and the Receiving PSP, with a default **50:50** split.
- Where stolen funds are recovered by the Receiving PSP, 50% of these funds must be repatriated to the sending PSP.
- Reputational damage is a large risk, especially due to the requirement on 14 of the largest PSPs to collect APP fraud data and provide it to the regulator who will then **publish** it.
- **Who** must be reimbursed:
  - consumers (individuals who are acting for purposes other than a trade, business or profession);
  - micro-enterprises (enterprises that employ fewer than 10 people and whose annual turnover and/or annual balance sheet total does not exceed £2m); and
  - charities (as defined in the relevant legislation and with annual income of less than £1m).

Strategy to reduce APP

- **Detect and prevent**
  - Implement capability to identify customers and transactions with higher risk of APP fraud.
  - Develop detailed descriptions of the threats targeting customers, and use this to drive your processes around what you deploy to protect which customers and how.
  - Align and schedule customer awareness initiatives to the threats and most appropriate timings.
  - Apply expanded recipient account and off-book profiling for mule targeting.
  - Implement Confirmation of Payee (if not already done).
  - Apply additional measures to protect vulnerable customers.
  - Review current standard of customer due diligence.
  - Use currently available shared intelligence sources and industry fraud databases.
  - Implement appropriate policies and processes to manage higher risk accounts.
- **Reimburse**
  - Implement appropriate governance, policies, processes, and controls for:
    - effective risk management to ensure PSP's adherence to reimbursement requirements,
    - amended complaints management process,
    - training staff responsible for assessing reimbursement request cases (including training on identifying vulnerable customers),
    - workflow/case management implemented with integration to customer record to ensure a single source of the truth,
    - suitable and comprehensive customer communications.
- **APP fraud aftermath**
  - Implement robust mechanisms for identifying and freezing funds received as a result of an APP fraud and, where appropriate, repatriate them.

https://kpmg.com/uk/en/blogs/home/posts/2023/06/app-fraud-publication.html

An ecosystem problem



According to National Cybercrime Reporting Portal (NCRP), victims of digital financial fraud lost **₹10,319 crore** in more than **694,000 complaints.**

Do I have any recommendations?

Ross Anderson on Economics of Security

- **Public goods**: non-rivalrous (my using them doesn't mean there's less available for you) and non-excludable (there's no practical way to exclude people from consuming them).
- **Uncoordinated markets** are generally unable to provide public goods in socially optimal quantities.
- Public goods may be supplied by **governments** directly, as in the case of national defense, or by using indirect mechanisms to coordinate markets.
  - I do not have an anti-aircraft gun on the roof of my house; air-defense threats come from a small number of actors, and are most efficiently dealt with by government action.
- So what about Internet security? Certainly there are **strong externalities** involved, and people who connect **insecure machines** to the Internet end up dumping costs on others, just like people who burn polluting coal fires. https://www.cl.cam.ac.uk/~rja14/book.html

Design principles

- Responsibility for solving the problem should be cast on the party **best placed** to fulfil it.
- Recognition of some customers as **vulnerable** will help devise appropriate controls.
- Without different stakeholders **sharing** information, the problem is unlikely to be solved.
- If the problem persists, it will affect **trust** in digital payments.
- **Disclosures** and transparency need to be prescribed and validated.
- A well-defined **taxonomy** is required to define and measure payment fraud.
- It is important to keep the **customer** at the centre.

“The real voyage of discovery consists not in seeking new landscapes, but in having new eyes.”

— Marcel Proust

Click below to connect...

@saravade

https://in.linkedin.com/in/saravade

advisory@saravade.in