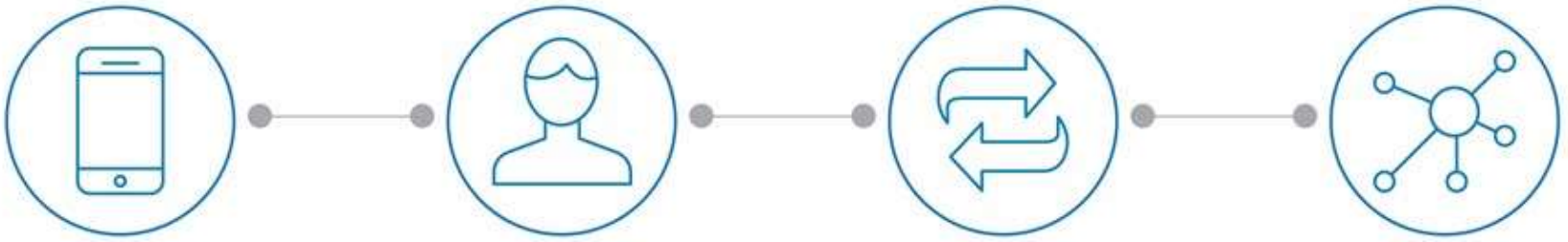
Digital frauds

SIRC of ICAI

13th January, 2020

Digital Vulnerability



DEVICE

USER

TRANSACTION

NETWORK

ACCESS POINTS

to digital business including mobile devices and PCs through diverse touchpoints: apps, mobile & desktop browsers

DIGITAL IDENTITY

User validation and online authentication to determine whether users are who they claim to be

ONLINE ACTIVITY

Analysis of transactional data related to specific activities e.g registration, purchase, payment, money transfer

COLLECTIVE INTELLIGENCE

Add external data from data pools and networks to your support your own analysis

Small – Digital fraud

Cases where amount involved is ₹1 lakh and above

Year	■ No. of frauds	Amount involved (₹ crore)
2016-17	1,372	42.29
2017-18	2,059	109.56
2018-19	1,866	71.38
Cases where amount involved is below ₹1 lakh		
2017-18	32,732	59.43
2018-19	50,438	78.04

Bank Frauds

Bank Group/ Institution	2017-18		2018-19	
	Number of Frauds	Amount Involved (₹ million)	Number of Frauds	Amount Involved (₹ million)
1	2	3	4	5
Public Sector Banks	2,885	382,608.7	3,766	645,094.3
	(48.8)	*(92.9)*	*(55.4)*	*(90.2)*
Private Sector Banks	1,975	24,782.5	2,090	55,151.4
	(33.4)	*(6.0)*	*(30.7)*	*(7.7)*
Foreign Banks	974	2,560.9	762	9,553.0
	(16.5)	*(0.6)*	*(11.2)*	*(1.3)*
Financial Institutions	12	1,647.0	28	5,534.1
	(0.2)	*(0.4)*	*(0.4)*	*(0.8)*
Small Finance Banks	65	61.9	115	75.2
	(1.1)	*(0.0)*	*(1.7)*	*(0.0)*
Payment Banks	3	9.0	39	21.1
	(0.1)	*(0.0)*	*(0.6)*	*(0.0)*
Local Area Banks	2	0.4	1	0.2
	(0.0)	*(0.0)*	*(0.0)*	*(0.0)*
Total	**5,916**	**411,670.4**	**6,801**	**715,429.3**

Fraud Management

Service Subscription

Identity Validation

Location
Velocity
Type of threat

Evaluation

Behavioral Analytics
Machine Learning

Recommended Actions

Predictions
Scoring Models
Case classification

Digital Identity Validation

Multi-Factor Authentication

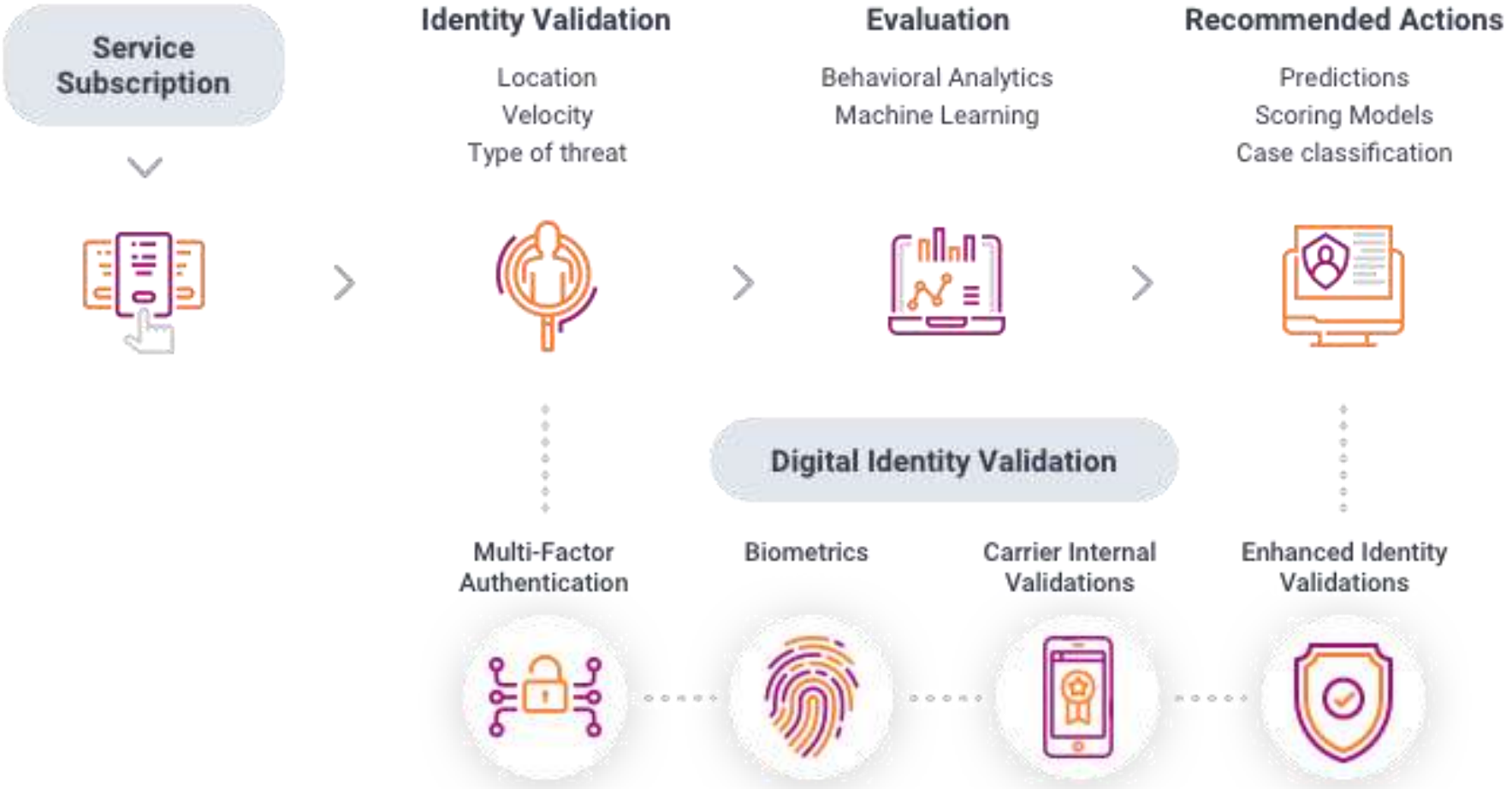
Biometrics

Carrier Internal Validations

Enhanced Identity Validations

Bank Frauds

Fraud management



Case studies

1. The remote access mobile application scam

Modus operandi

- Fraudsters, who had listed fake numbers online under an NGO's name, gained access to a Mumbai resident’s debit card details by asking her to download Anydesk, a remote desktop software tool, which provides a third party a complete view of the user’s screen. She wanted to transfer funds to the NGO to cremate her pet. Instead, her debit card details were compromised and Rs 30,000 was withdrawn from her bank account ..

  Lessons to learn
  Do not seek help from strangers to complete payment transactions.
  Do not download apps, except official ones, recommended by seemingly-helpful people, even if they claim to be bank staff.

2. Trap for gullible insurance seekers

- **Modus operandi**
  In this, scammers prey on an individual's inability to spot the difference between the official and fake portals of the insurance regulator. A counterfeit portal going by the URL www.irdaionline. org managed to sell fake policies to insurance seekers until the IRDAI issued an alert, and the URL was blocked.

  Lessons to learn

  Irdai does not sell insurance policies. Stay away from portals misusing domains that are akin to regulators' official ones to swindle funds.

3. Phishing SMS messages promising income tax refund

- **Modus operandi**
  A Mumbai-based private sector employee received a link, purportedly from the income tax department, regarding a tax refund he was eligible for. Once he clicked on the link, he was directed to a mobile application that got downloaded on his phone. Tricksters elicited his account access details and siphoned off money.

  Lessons to learn
  The income tax department directly credits the refund to the bank account mentioned in your I-T return form. Do not trust any messages, links, online forms or calls seeking additional account/card details.

4. The KYC update hoax

- **Modus operandi**
  An IAS officer in Udaipur lost Rs 6 lakh when she clicked on a fraudulent link asking her to update her KYC. She was prompted to enter her account details and the OTP received, following which she received messages from her bank notifying her of debits worth Rs 6 lakh.

  Lessons to learn
  Do not click on links received through SMS messages. Rely on official websites or bank branches to complete the process, if required

5. Simple to crack passwords

- **Modus operandi**
  Here, victims make hacking an effortless job for hackers. The United Kingdom's National Cyber Security Centre (NCSC) recently released a list of 'most hacked' passwords. Over 23 million accounts worldwide were breached as they had 123456 as their passwords.

  Lessons to learn
  While the data pertains to the UK, it is a pointer to the hazards of using passwords and PINs that are easy to decode.

6. Fake UPI-based payment links

- **Modus operandi**
  Fraudster asked the victim, a Pune-based trader, to transfer a nominal amount of Rs 10 to a mobile number from his digital wallet. It was presented as ‘registration fee’ to initiate the online purchase of a scooter. Subsequently, he received payment links where he had to enter his UPI ID and OTP received and send it back to the fraudster. The information was used to transfer Rs 1.53 lakh out of his accounts.

  Lessons to learn
  Transact only through the official BHIM or bank UPI apps. Do not use links sent by unknown entities, even if they seem authentic.

7. Fraudulent NPCI/UPI/BHIM handles and portals

- **Modus operandi**
  Myriad Twitter handles masquerading as @NPCI_BHIM official helpline handle have mushroomed on the micro-blogging site. The fake accounts trick customers looking for help to reveal their account, wallet or card details.

  Lessons to learn
  Look for verified-by-twitter blue ticks while interacting with National Payments Corporation of India (NPCI), bank or payment wallet helplines.

8. Lack of awareness of UPI pay options

- **Modus operandi**
  A Pune resident who wished to sell his air-cooler was tricked by a prospective buyer who agreed to pay `9,000 through a UPI-based app. However, the latter sent a ‘pay’ request to the former, who promptly authorised it without realising that the amount would be debited from, not credited to, his account.

  Lessons to learn
  Use of newer technologies calls for additional caution. Since UPI-based apps enable push (pay/send) and pull (receive/collect) transactions, newer users could get confused. Understand the processes thoroughly before rushing to use them.

8. Lack of awareness of UPI pay options

- **Modus operandi**
  A Pune resident who wished to sell his air-cooler was tricked by a prospective buyer who agreed to pay `9,000 through a UPI-based app. However, the latter sent a ‘pay’ request to the former, who promptly authorised it without realising that the amount would be debited from, not credited to, his account.

  Lessons to learn
  Use of newer technologies calls for additional caution. Since UPI-based apps enable push (pay/send) and pull (receive/collect) transactions, newer users could get confused. Understand the processes thoroughly before rushing to use them.

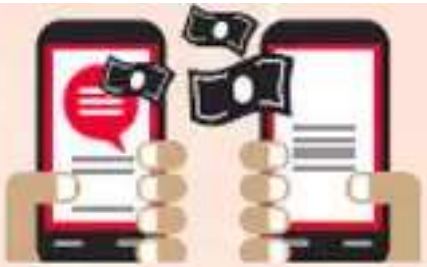
9. COSMOS Bank

- **Modus operandi**

In two days, hackers withdrew a total Rs 78 crore from various ATMs in 28 countries, including Canada, Hong Kong and a few ATMs in India, and another Rs 2.5 crore were taken out within India.

PNB SWIFT Interface

What The Panel Suggests



Create level playing field between banks & non-banks to expand digital payments

Encourage entry of fintech firms dealing in fraud control

Reform P2P system to develop marketplace model of lending

Push virtual banking

Convert small savings schemes into demat

Liberalise use of prepaid instruments

Consider video-based KYC, use of DigiLocker

Use unconventional data to reach the unbanked

Use blockchain, AI for credit, drones for crop insurance

Make govt data available through open APIs

Create task force in [illegible] for data protection

5 WAYS TO PREVENT DIGITAL FRAUD IN BANKS

1 BLOCKCHAIN

Blockchain enables these businesses to create an unchangeable, replicated, and distributed database that reduces fraud by giving real-time transparency into how the data is being used across the network.

2 A COMPREHENSIVE RISK MANAGEMENT MODEL

A best-in-class risk management program should look at all types of risk across the business including Market Risk, Credit Risk, Operational Risk and Finance/Treasury/Accounting Risk.

3 DIGILOCKERS – THE DIGITAL INDIA INITIATIVE

It is a document storage, verification, and utility service. The move is A to eliminate the need for physical copies of important documents and to encourage digital processing of document-related tasks.

4 SINGLE-SIGN-ON (SSO)

In order to avoid a data breach, it is important for financial institutions to focus on maintaining the security of client's confidential information. Adhering to privacy laws will remove the stress of getting into a legal fuss.

5 DATA PROTECTION STRATEGY

Data serves as the oil that is running the wheel of current digital businesses. So, data protection strategy that has factors such as data privacy, data security, data lineage, data governance and more should be a top priority for banks.

DQINDIA