Fool me once - Learning from the IMPS Glitch

By Nandkumar Saravade[1]

The Italians having a Proverb, He that deceives me once, it s his fault; but if twice, it s my fault.'" - Anthony Weldon (1651), The Court and Character of King James

1. What happened?

On 15 November 2023, UCO Bank reported[2] to the National Stock Exchange (NSE) that during the period from 10 November to 13 November, due to technical issue in Immediate Payment Service (IMPS), certain transaction(s) initiated by holders of other banks had resulted in credit to the account holders in UCO Bank without actual receipt of money from these banks. The Bank, as a precautionary measure had made the IMPS channel offline and was working closely with the stakeholders to resolve the issue and restore the IMPS services at the earliest. The matter was also reported to the law enforcement agencies for necessary action.

In a follow-up filing dated 16 November 2023,[3] the Bank informed: "…by taking various proactive steps, Bank blocked the recipients 'accounts and has been able to retain and recover around ₹649 crore out of ₹820 crore which is about 79% of the amount."

Subsequently, on 5 December[4], the Central Bureau of Investigation (CBI) which initiated investigation into the matter released a press note, as follows.

A case was registered on complaint from UCO Bank, against two Support Engineers working with UCO Bank and other unknown persons on the allegations of suspicious Immediate Payment Service (IMPS) transaction amounting to approximately ₹820 crore.

It was alleged that between 10th November 2023 and 13th November 2023, IMPS

[1] Former IPS officer and Co-founder, DeepStrat

[1] https://nsearchives.nseindia.com/corporate/UCOBANK_15112023091630_nsebse.pdf

[2] https://nsearchives.nseindia.com/corporate/UCOBANK_16112023091244_exchange.pdf

[3] https://cbi.gov.in/press-detail/NjAwMQ==

inward transactions originating from 14000 account holders across seven private banks were directed to 41000 account holders within UCO Bank through the IMPS channel. It was further alleged that this intricate network involved a staggering 8,53,049 transactions and these transactions were mistakenly posted in the UCO Bank account-holders' records, despite the originating banks registering failed transactions. Consequently, an approximate sum of ₹820 crore was allegedly found its way into UCO Bank accounts without proper debits from the originating banks' account holders.

It was also alleged that several account holders exploited this situation, illicitly withdrawing funds from UCO Bank through various banking channels, thereby benefiting wrongfully from the transaction."

Apparently, the news about the glitch was shared on social media and exploited by those who came to know of it. One such video can still be seen on YouTube.[5]

2. How is this a criminal case?

Some people have asked this question: Should bank account holders who happen to see undue credits in their accounts and proceed to withdraw the money, be treated as debtors or criminals? The law is very clear on this point. Section 403 of the Indian Penal Code deals with 'dishonest misappropriation of property. 'An explanatory clause states as follows.

A person who finds property not in the possession of any other person, and takes such property for the purpose of protecting it for, or of restoring it to, the owner, does not take or misappropriate it dishonestly, and is not guilty of an offence; but he is guilty of the offence above defined, if he appropriates it to his own use, when he knows or has the means of discovering the owner, or before he has used reasonable means to discover and give notice to the owner and has kept the property a reasonable time to enable the owner to claim it."

I have known of two instances when this section had to be invoked. In one case, in olden days, a bank while issuing the cheque for a matured fixed deposit, made an error of missing the decimal point, with the result that the amount was 100 times more than the correct one (close to a crore of rupees). The recipient realised the situation and withdrew the amount. It was after the threat of legal action that he refunded the excess amount.

In another instance, a software upgrade resulted in ATM withdrawals in Eurozone to be dispensed in Euros, but the account would get debited in rupees.

[5] https://youtu.be/bzvFAkVqWgE

An Indian account holder who happened to be traveling in Europe realised the 'opportunity 'and proceeded to withdraw almost ₹70 lakh in local currency. It required a strong follow up by the concerned bank's fraud management team to file an FIR and get the money back.

The principle of *no one being entitled to undue benefit at another s cost* is very much in action in the current instance also.

3. Why should the buck stop right at the top?

There is an old saying: *Soldiers do not lose wars; wars are lost by generals.* For any event to turn catastrophic, the lack of foresight and preparedness by past and current leaders is responsible.

Let's look at the issue of governance in public sector banks (PSBs). The definitive study report[6] on this was written by a distinguished committee headed by P J Nayak. A parliament question response[7] by the Finance Minister on 1 August, 2014 summarised the recommendations well: "The main recommendations of the Committee, inter alia, relate to elimination of dual control over Public Sector Banks (PSBs), upgradation of the quality of Board deliberation, setting-up of a Bank Investment Company (BIC) and reducing Government's stake in PSBs to less than 51%, uniform licence regime across all broad based banks, selection of top management of bank by Banks Board Bureau and subsequently by BIC and then Banks' Board."

A decade down the line, many of the recommendations have not been acted upon. The quality of boards in many (but not all) PSBs in particular remains a weak area.

RBI had recognised the need for specialised technology experience and oversight in the Board of Directors. The report of the G Gopalakrishna Working Group[8] on on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds, of which I was privileged to be a member, was published on 21 January 2011. It had a chapter on IT Governance. One of the recommendations in the report was as follows.

A qualified and an independent IT Strategy Committee should be set up with a minimum of two directors as members, one of whom should be an independent director. IT Strategy Committee members should be technically competent. At least

[4] https://www.rbi.org.in/scripts/PublicationReportDetails.aspx?UrlPage=&ID=784
[5] https://eparlib.nic.in/handle/123456789/669861?view_type=browse
[6] https://m.rbi.org.in/scripts/PublicationReportDetails.aspx?UrlPage=&ID=609

one member should have substantial IT expertise in managing technology."

While the WG recommendations were not binding, subsequently RBI reiterated these expectations about expert oversight, culminating in the recent Master Directions[9] issued on 7 November 2023, which have laid down timelines for all Regulated Entities (REs) to abide by the provisions of the IT Strategy Committee of the Board (Clause 6) and the relevant processes which they should follow. These include REs establishing a Board-level IT Strategy Committee (ITSC) with three members, with an independent director having substantial IT expertise in managing/ guiding information technology initiatives as the chairperson.

A cursory perusal of the UCO Bank website failed to reveal any board member who seemed to have significant technology experience. I will be happy to be proved wrong on this assumption.

4. What processes seemed deficient?

Bankers will realise that one important aspect of the glitch was that it continued for three days. The efficiency of the Bank in reconciling various systems (as measured by Turn Around Times (TATs)) is not known, but more prompt **reconciliation** could have detected the mismatch and mishap. Apparently, the relevant IMPS transaction data is shared across the platform by the National Payment Corporation of India (NPCI) every four hours. So, in an ideal world, with robotic process automation (RPA) etc, the red flag would have been up in a matter of hours. Perhaps, the timing of the glitch (11 November being second Saturday and 12 December being Sunday/Kali Puja) may have acted as the delaying element. It remains to be seen if this was happenstance or was a deliberate choice by someone.

Another way to detect the anomalous transactions was by having an effective **fraud monitoring** system. Just look at the numbers.

- Originating accounts: 14000 (across seven private banks)
- Destination accounts: 41000 (within UCO Bank)
- Number of transactions: 8,53,049 (almost 21 per account)
- Prompt withdrawal from these 41,000 accounts

Any fraud monitoring team worth its salt would have caught the trends very quickly. Now, it is well known within the industry that PSBs lack dedicated and skilled centralised fraud management teams. Software purchased at great expense lies underutilised due to this missing skillset.

[7] https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12562

The third aspect of process gaps appears to be **change management** of software configurations/new application versions. Investigation by CBI should reveal whether the configuration changes (or else) which led to the glitch were authorised/conscious or inadvertent. However, the right change management process under IT governance seems lacking.

Let's see what RBI has prescribed in the latest Master Directions, referred to above.

13. Change and Patch Management

REs shall put in place documented policy(ies) and procedures for change and patch management to ensure the following:
(a)the business impact of implementing patches/ changes (or not implementing a particular patch/ change request) are assessed;
(b)the patches/ changes are applied/ implemented and reviewed in a secure and timely manner with necessary approvals;
(c) any changes to an application system or data are justified by genuine business needs and approvals supported by documentation and subjected to a robust change management process; and
(d)mechanism is established to recover from failed changes/ patch deployment or unexpected results.

It is thus clear that all changes need to be done as a part of larger plan and with due oversight. The guide[10] published by the Cybersecurity and Infrastructure Security Agency (CISA) of the US Government has recommended the guidelines published by the Carnegie Mellon University about change management. Among other things, it recommends a "configuration control review board (CCRB)—an organizational construct, made up of stakeholders, that is responsible for supporting the assessment, prioritization, authorization, and scheduling of changes to Configuration Items and the implementation of policies governing those changes. ITIL refers to this construct as a Change Advisory Board." It is not known if such an oversight team exists in UCO Bank and how effective it is.

It is also not known if the configuration error emanated out of defective code (which would reflect on the User Acceptance Test process), or parameter changes (which would indicate faulty architecture). Coverage by Privilege Access

[8] https://www.cisa.gov/sites/default/files/c3vp/crr_resources_guides/CRR_Resource_Guide-CCM.pdf

Management tools may also be relevant to examine.

A more subtle point: I have heard knowledgeable banking practitioners talk about the absence of adequately knowledgeable maker-checkers, who should be bank employees and not vendor staff, in a 24x7 payment environment. Ideally, with burgeoning data centre operations and round -the-clock availability of payment infrastructure (including NEFT/RTGS), this should have been in place already. Perhaps, a time has come for banks to over-invest in these areas.

5. Cybersecurity is an ecosystem responsibility

An influential paper[11] titled "Cyber Risk, Market Failures, and Financial Stability" published by IMF in April, 2017 rightly identified that "the true aggregation of risks related to cyberspace goes well beyond the internal monitoring and risk management capacities of an individual institution." No single organisation, however well-resourced, can hope to be successful on its own, and has not only to work with its peers to be on top of threat intelligence and share best practices on cyber resilience, but also will need to rely on the regulator, law enforcement and national security institutions to protect its assets and customers.

So, what is India's record in strengthening the ecosystem?

In January 2017, the Financial Stability and Development Council, chaired by the then Finance Minister, had resolved to set up a Computer Emergency Response Team in Financial Sector (CERT-Fin) to work towards strengthening cyber security of the sector. Accordingly, a working group was set up, of which I happened to be a member. The detailed report of the working group was published[12] on 30 June, 2017.

The key recommendations of the report included CERT-Fin to be set up as a not-for-profit company and act as an umbrella CERT, with sub-sectoral CERTs (separately dealing with banking, markets, insurance and pension), housed in each of the financial sector Regulators. An important recommended function CERT-Fin was to develop was on cyber skills and to promote information sharing among the industry participants.

It should be a matter of national concern that CERT-Fin never took off, probably due to some confused thinking in Ministry of Finance. This important piece of the puzzle where a mechanism for documenting major cyber incidents, culling out

[9] https://www.elibrary.imf.org/view/journals/001/2017/185/001.2017.issue-185-en.xml
[10] https://dea.gov.in/sites/default/files/Press-CERT-Fin%20Report.pdf

their learnings and propagating them in the financial community in a structured manner - to avoid same mistake being committed due to **lack of institutional memory** - has remained missing.

Has an incident like UCO Bank happened before? It has. In a report published in Livemint[13] on 30 March, 2017, it was reported that Bank of Maharashtra lost ₹25 crore in one of the biggest Unified Payments Interface (UPI) frauds till then - when a few people moved money illegally, taking advantage of a minor bug. The bug in the UPI system allowed people to send money without having the necessary funds in their accounts. Even when the core banking solution of the bank declined a transaction, the UPI solution used to send the success message to NPCI. About 50-60 people in Aurangabad discovered this loophole, possibly through a trial-and-error method.

Similar issues of inadequate software testing and change management and lack of timely reconciliation were flagged in that case as well.

It is clear that many of the financial and other institutions have to up their game to ensure that such large incidents (whether out of negligence or malice) are prevented. It is everyone's responsibility to protect the trust in electronic banking and Digital India.

6. Summing up

One poet has said that no one learns without a trauma.

Kaun seekha hai sirf baton se, Sabko ek hadsa zaroori hai." -- Jaun Elia

Another poet (Sahir Ludhianvi) has elaborated further.

कभी ख़ुद पे, कभी हालात पे रोना आया । बात निकली तो हर एक बात पे रोना आया ॥
कौन रोता है किसी और की ख़ातिर, ऐ दोस्त ! सब को अपनी ही किसी बात पे रोना आया ॥
(One despairs sometimes at own shortcomings, sometimes at the adverse circumstances. No one laments for another, the empathy is for one's own misfortunes)

In general, individual learning is experiential, but organisations do not have the same luxury. Even in a fiercely competitive environment, with adaptive

[11] https://www.livemint.com/Industry/8HUcQEUGBn0CcPOD6cbfJP/Bank-of-Maharashtra-accounts-lost-Rs25-crore-due-to-UPI-bug.html

adversories whose numbers and reach can scale up scarily, collaborating with peers and learning from others' failures becomes imperative.

Risk managers and business leaders owe it to their profession, customer and shareholders to be up to the job, and not let public funds be taken away with impunity. The ecosystem operated by the government and the regulators should enable and empower them with the right policies and shareable knowledge.

Disclaimer: I have attempted to compile some stray thoughts on the incident, based on what appeared in public domain. I will be happy to be corrected on any factual gaps and wrong assumptions. Please reach out at advisory@saravade.in