AIBEA's Banking News

15 JULY 2017

NEWS BULLETIN FROM ALL INDIA BANK EMPLOYEES' ASSOCIATION

Deposited demonetised notes still being counted: RBI Governor

RBI governor Urjit Patel appeared before the Standing Committee on Finance on Wednesday

HIGHLIGHTS

- **RBI Governor Urijit Patel has said that the amount of junked notes deposited after demonetisation was still being counted**
- **He said the total money in circulation in the country now was Rs 15.4 lakh crore against Rs 17.7 lakh crore at the time of demonetisation**

TIMESOFINDIA.COM | Jul 12, 2017

THE TIMES OF INDIA

NEW DELHI: RBI Governor Urijit Patel on Wednesday told a parliamentary committee that the amount of junked notes deposited after demonetisation was still being counted.

Patel gave this information at a meeting of the Parliamentary Standing Committee on Finance when a member specifically asked him to give details of the value of the Rs 500 and Rs 1,000 notes which were allowed to be exchanged till December 30.

He said the total money in circulation in the country now was Rs 15.4 lakh crore against Rs 17.7 lakh crore at the time of demonetisation in November last year, according to sources.

At the meeting, Naresh Agarwal of the Samajwadi Party is understood to have demanded the names of 12 industrialists whose outstanding loans amounted to 25 per cent of the non-performing assets in the banking system.

Naresh Agarwal and Trinamool Congress MP Saugato Roy had previously asked the RBI Governor how much of the banned notes have come back into the system. The RBI governor said the total money in circulation now is Rs. 15.4 lakh crore against Rs. 17.7 lakh crore in November last year when Prime Minister Narendra abruptly banned high value notes in an attempt to battle black money and corruption.

The Standing Committee on Finance headed by Congress leader Veerappa Moily had also questioned RBI governor, on the decision of demonetisation, on January 18 as well but most of their questions had remained unanswered then.

Vijay Mallya extradition: British courts' swift delivery may help

For Mallya, who may claim "political witch-hunt" as his defence, the Indian investigative agencies plan to highlight his alleged money laundering activities as he stands accused of defaulting on bank loans of Rs 9,000 crore

BY RAGHAV OHRI | JUL 12, 2017

THE ECONOMIC TIMES

NEW DELHI: It took the British Supreme Court all of 81 days to rule in January that Parliament alone had the right to trigger Brexit, dashing Prime Minister Theresa May's hopes of starting the process of Britain's withdrawal from the European Union without the intervention of MPs and their peers.

Businessman Vijay Mallya, who is facing extradition from Britain over unpaid loans taken for the defunct Kingfisher Airlines, however, appeared not to have taken the swift pace of the British delivery system into account when he told Indian media persons in London last month to "keep dreaming about a billion pounds".

Unlike Indian courts, where a litigation can be stretched for years, the British justice dispensation system has little room for such manipulation. With the British Crown Court fixing December 4 as the final hearing date in Mallya's extradition case, the verdict is highly unlikely to be delayed beyond February 2018, according to British barristers.

Add to it a minimum of six months and a maximum of one year for the British High Court, the appellate court, to decide on the appeal against the decision of the Crown Court, they said. And similar is the time, perhaps less, that the British Supreme Court is expected to take to decide the fate of the former liquor baron.

That is, except if the Indian investigative agencies produce some "fresh evidence" against Mallya, which may lead to a delay, although an insignificant one, in the proceedings.

Extradition is fundamentally a "short trial" where unlike a normal trial witnesses ought not to be produced. The decision whether to extradite depends on the "evidence" and records produced by the prosecuting agency, and the court is required to reach a prime facie conclusion whether to order extradition of the individual in question.

The final say, going by the rulebook, rests with the British government, which has the power to retain an individual despite the order of the country's highest court. However, according to experts, this is highly unlikely in cases of economic offence.

An exception may be made in a case where a person is accused of committing a political offence, unlike Mallya, who stands accused of money laundering, duping banks, and cheating, among other criminal offences.

For Mallya, who may claim "political witch-hunt" as his defence, the Indian investigative agencies plan to highlight his alleged money laundering activities as he stands accused of defaulting on bank loans of Rs 9,000 crore. With Prime Minister Narendra Modi seeking his British counterpart's help earlier this week for the return of economic offenders, the Indian side is working hard to make a solid legal case for the Crown Prosecution Service.

India has had a dismal record when it comes to Britain allowing its extradition requests. Of the several requests India has made to the British since 1992, only one has fructified so far, perhaps a reason for Mallya to smile.

With two charge sheets already filed against him, by the CBI and Enforcement Directorate, Mallya may face further legal trouble though as agencies are busy digging dirt against him in another case registered against him on the complaint of the State Bank of India. Besides, as ET had first reported, the involvement of as many as 23 banks in doling out loans without any securities to Mallya is under the scanner.

Bank of Baroda moves NCLT to recover Rs97 crore from Binani Cement

Bank of Baroda invoked the Insolvency and Bankruptcy Code on Binani Cement after the firm failed to come up with a restructuring plan to recover the loans

Lawyers for Binani Cement claim Bank of Baroda's application had several technical flaws, and that its claim was minuscule compared with the total value of the group's assets, which, according to its lawyers, is Rs14,000 crore

Arkamoy Dutta Majumdar/ LIVEMINT

Kolkata: Bank of Baroda has filed a petition against Binani Cement Ltd with the National Company Law Tribunal's (NCLT) Kolkata bench, seeking to recover Rs.97 crore in an outstanding loan under the new Insolvency and Bankruptcy Code after the firm failed to come up with a restructuring plan to clear its dues.

Lawyers for Binani Cement, a privately held firm of the Braj Binani Group, claimed Bank of Baroda's application had several technical flaws, and that its claim was minuscule compared with the total value of the group's assets, which, according to its lawyers, is Rs14,000 crore.

Binani Cement, which is a unit of Binani Industries Ltd, had assets worth Rs5,074.83 crore at the end of March, according to the holding firm's auditor, MZSK & Associates.

NCLT's Kolkata bench on Wednesday reserved its order on whether or not it would admit the lender's application under the new insolvency code. If the application is admitted, the company's board will be superseded and an interim resolution professional appointed to take control of its assets and operations. Bank of Baroda wants management consulting firm Deloitte to be appointed as interim resolution professional.

Pratap Chatterjee, counsel for Binani Cement, said Bank of Baroda was not the lead lender to the cement maker and that it had not taken the approval of the joint forum of lenders before moving NCLT. Citing Reserve Bank of India rules, Chatterjee said Bank of Baroda was required to write to the joint forum and wait for at least 30 days before unilaterally moving NCLT.

Chatterjee asked why Bank of Baroda was seeking the appointment of an administrator to recover a small loan of Rs97 crore when the lead banker, Central Bank of India, was not seeking dispute resolution in this manner.

However, senior advocate Ratnanko Banerjee told the bench that Bank of Baroda's move had the backing of the joint forum of lenders led by the Edelweiss Group, and that Binani Cement was in distress because the management had failed to come up with a restructuring plan.

Bank of Baroda has in its application said the firm had in a meeting with the joint forum of lenders in January committed to preparing a restructuring plan, according to the bank's counsel, Rishav Banerjee. Lenders met the management again in April, but no concrete plan for revival has yet been given, Banerjee said in his submission to the bench.

In fiscal year 2016-17, Binani Cement registered a net loss of Rs349.31 crore on revenue of Rs1,534.62 crore, according to the auditor of its holding company. Binani Industries' net consolidated loss was Rs468.37 crore, and its consolidated liabilities exceeded its assets by Rs1,525.32 crore.

"The management has represented to us that it is hopeful of revival of businesses in the subsidiaries in the near future," auditor MZSK & Associates wrote in its report.

Lenders, however, appear to have lost confidence in the management. Banerjee said Bank of Baroda had lent Rs386 crore in all, and that Rs97 crore is currently outstanding. The company started to default on its repayment obligations in 2015, he added.

Just hit reply: RBI to banking customers

The RBI has issued a notification to make banks more responsive in protecting customers from fraudulent banking transactions

You would be able to reply to transaction notifications to raise a fraud alert; iStock

Vivina Vishwanathan livemint

Did you know that every time you swipe a card, you may be exposing yourself to a hacker or a fraudster? Recently the Reserve Bank of India (RBI) said that there has been a surge in grievances relating to unauthorised transactions. In 2016, banks reported multiple instances of data breaches, especially with debit and ATM cards. In 2013, too, banks had reported several instances where Indian credit cards were used fraudulently from websites overseas—while, even today, many online fraudulent transactions remain unreported. However, that doesn't mean you should stop electronic transactions.

To ensure that banks provide more protection to customers' electronic transactions, last week the regulator issued a notification on customer protection in case of electronic banking transaction. You can read it **here**.

In the notification, RBI clearly spelt out banks' as well as customers' liabilities in case of unauthorised electronic banking transactions. Here is what it means for you.

Quick response

Imagine you get a message from your bank saying Rs25,000 is debited from your account. However, you didn't do the transaction. Your immediate response may be to call your bank, send an email or maybe even visit a branch.

The RBI's notification wants banks to provide more options for reporting fraudulent transaction immediately. For instance, today when you get an SMS or an email about a transaction, you cannot reply to it. The RBI has asked banks to enable services so that customers can instantly respond by replying to the SMS or email alerts they get from banks. Soon you may be able to respond instantly to any SMS that you believe could be about a fraudulent transaction. The regulator has also asked banks to provide a direct link for lodging complaints, with a specific option to report unauthorised electronic transactions on the home page of banks' websites. Currently, you don't have this option on the home page. "For the things that RBI has listed, all banks will have to work with their core banking teams that looks at protocols on intimations. We also have to give details to the vendors. Hence, it will take time for banks to make these changes," said Puneet Kapoor, senior executive vice president, Kotak Mahindra Bank Ltd.

Reporting timeline

Reporting a fraud is the first step to dealing with it. The regulator has given a structure on how to do it. Bankers say that these reporting requirements existed earlier also but now there is a standard time frame for reporting them, and your liability is linked to the timeline.

To begin with, if an unauthorised transaction takes place and the bank is responsible for it, then even if the customer doesn't report the fraud, the customer has zero liability. This means the bank will make good any losses you may incur. "Most banks take an insurance on fraudulent attacks such as skimming and hence the customers' liability too gets limited when it gets reported," said Sangram Singh, head-cards and payments business, Axis Bank Ltd.

Now, say there is a third-party breach where neither the bank nor the customer is responsible and the customer responds within 3 working days. Then too the customer doesn't have any liability. But in case you don't report the fraud within 3 days but within 4 to 7 working days after receiving the communication from the bank, you will have limited liability for the transaction. Limited liability means you will incur some monetary loss for the fraud.

But what if you report after 7 days? In such a situation the bank will decide what to do. While these policies will vary from bank to bank, all banks have been asked to put details of their policy in the public domain and also inform customers about it individually. Remember that the above timeline starts after the day complaint was made. And the working days are counted based on the schedule of the home branch. Also, once reported, the RBI has asked banks to resolve the case within 90 days from the date of receipt of the complaint.

The cost

In cases where you share responsibility for a fraudulent transaction, or you have limited liability due to late reporting, the central bank has listed out the liabilities in detail. If the loss is due to your negligence, you bear the entire loss till the time it was reported to the bank. For instance, if you have shared your PIN or password with anyone and the money was stolen, you have to bear the loss. But even in such cases, any loss occurring after the reporting of the unauthorised transaction will be borne by the bank. Wherever you have limited liability, the amounts have been capped in the range of Rs5,000-25,000. The amount depends on the kind of account you use. For instance, for a basic savings account, the liability is capped at Rs5,000. For other savings accounts, prepaid instruments, gift cards, and credit cards with limits of up to Rs5 lakh, your liability is limited to Rs10,000. For credit cards with limits above Rs5 lakh, liability is capped at Rs25,000.

Now, what happens to the money that gets lost due to the fraudulent transactions? Once you inform the bank, the bank has to credit the amount involved in the unauthorised electronic transaction to your account within 10 working days from the date you raise the alert. In case of debit card or bank account fraud, the customer does not suffer loss of interest. In case of credit cards, the customer does not bear any additional burden of interest.

What you should do

Just because roads are prone to accidents, do you stop driving on the road? To avoid accidents, you take safety measures and follow the rules. Similarly, you should protect yourself from frauds in case of online transactions.

How can you do this? If you use online transactions or swipe cards, you should sign up for all the SMS and email alerts for electronic banking transactions. This is the easiest way to know if there has been any movement in your account. In case of any unauthorised transaction, you should immediately inform your bank. When you register a complaint, banks record its time and date, which is important to determine the extent of your liability. Hence, ensure that you don't delay the process.

Incentivising financial sector cybersecurity

Policy that offers the correct economic incentives for institutions to be proactive is as important as the technical aspects of cybersecurity

The Narendra Modi government's push for a less-cash economy is increasing the digital density of India's financial services space.

live mint

Two developments last week point to the evolving cybersecurity architecture in India's financial sector. First, the government made public a report by the working group established to help set up the Computer Emergency Response Team in the Financial Sector (Cert-Fin). Then, the Reserve Bank of India (RBI) released guidelines on customer liability in case of unauthorized electronic banking transactions. They represent different aspects of the cybersecurity problem—the technical and the broader economic framework. The latter deserves more attention than it has received.

The Narendra Modi government's push for a less-cash economy is increasing the digital density of India's financial services space. For instance, the government has targeted Rs2,500 crore worth of transactions via digital means such as the Unified Payment Interface, Aadhaar Pay and debit cards in FY18. More fundamentally, Modi's financial inclusion and development push, based on JAM (Jan Dhan Yojana, Aadhaar, Mobile connectivity), has digital underpinnings that mean potentially cascading effects if there are breaches in the financial sector.

The cyberattacks, meanwhile, have been getting audacious. Last year, a malware-related security breach compromised millions of debit cards that had to be blocked by the State Bank of India, HDFC Bank Ltd, ICICI Bank Ltd, YES Bank Ltd and Axis Bank Ltd. There was also the near-loss of $171 million, transferred via unlawful access to the Union Bank of India’s SWIFT codes.

New Delhi’s response thus far has focused on the technical aspects of the problem. That is necessary, certainly. There is a risk that Cert-Fin will become deadwood given that sectoral regulators RBI, the Securities and Exchange Board of India and the Insurance Regulatory and Development Authority of India are already working on cybersecurity issues. But if implemented well—as per the report, its role stretches from collection, analysis and dissemination of information regarding cyber incidents to monitoring the financial sector’s efforts to establish an effective cybersecurity architecture—it could enable coordination across the sector.

But no cybersecurity architecture can be foolproof for three reasons. First, when it comes to any reasonably complex system, attackers will always have the edge over defenders. Even if the former are poorly resourced and the latter have all the resources of a national government available to them, the number of potential bugs and vulnerable points in any system mean that the mathematical odds favour the attackers. Second, no code can be perfect enough to compensate for human error. In the Union Bank of India case, for instance, the attackers, posing as RBI officials, successfully phished a Union Bank staffer. And lastly, cybersecurity functions somewhat like herd immunity does for vaccinations. A bank might have robust cybersecurity architecture, but it will still be vulnerable if the systems of other networks that carry pertinent information are not secure. For example, the telecom sector is a potential avenue of attack when it comes to the financial sector.

That means that as much as technical measures, policy that offers the correct economic incentives for institutions to be proactive about cybersecurity, cooperate with the regulator and report breaches, is important. In a 2001 paper, *Why Information Security Is Hard—An Economic Perspective*, security engineering researcher Ross Anderson pointed out that in an international survey of ATM frauds, the US, where burden of proof lay with the banks, fared much better than Britain, Norway and the Netherlands, where burden of proof lay with the customer. The RBI’s guidelines on customer liability are welcome in this context.

What about liability for distributed denial of service (DDoS) attacks, now the most common kind of attack on financial institutions globally? Should dangerously unsecured networks, servers or Internet of Things devices that are infected and used to launch such attacks invite liability? Would that impose too heavy a regulatory burden and stifle business, or would it be positive inducement to be proactive in hardening cyber defences?

Then there is the software industry. From operating systems to security software, the first-mover advantage due to network effects—the more people use a particular software, the more valuable it becomes—has led to a "release first, patch later" approach. Should liability for companies that knowingly put out software with security holes be considered? It's a dicey proposition on the face of it—but as *The Economist* puts it, public opinion and governments are unlikely to be accommodating the first time a self-driving car causes an accident owing to a security breach.

Data breach disclosure norms, with penalties for failing to do so, are also important; they incentivise financial institutions to swiftly report cyberattacks instead of keeping mum to avoid reputation loss, regulatory intervention and liability. Many countries have such norms, but India does not. The RBI has mandated disclosure for banks, but deputy governor S.S. Mundra has admitted that many continue to suppress such information.

These are tricky issues. Going overboard with the regulatory burden and the negative effects of heavy-handed liability laws are both real dangers. But one thing is for certain: The tragedy of the commons dictates that companies and institutions will rarely expend the resources necessary for the collective security needed to protect the sector, until the right economic incentives are found.

AIBEA THIS DAY – 15 JULY

1953	**Justice Campbell Puri Tribunal appointed for Lloyds Bank dismissal cases.**
1957	**Bank Mazdoor Day observed to popularize our house magazine.**
1995	**National Convention of Mass Organisations against new economic policies meets at Delhi.**
1996	**Solidarity protest actions in support of struggles in Bharath Overseas Bank.**
2002	**National Assembly of Workers at Delhi against Government's anti labour policies; AIBEA participates.**