ALL INDIA UNION BANK PENSIONERS AND RETIREES FEDERATION
(Affiliated to All India Bank Pensioners & Retirees Confederation – AIBPARC)
163/4, Kutchery Road, Mylapore, Chennai - 600004
E mail i.d: aiubparf@gmail.com/ ubioatnngr@gmail.com/ **suryanarayananram@gmail.com**

Com. P.B. Thomas	Com. Nitin Desai	Com. S. Bagchi	Com. N. Govindarajulu
Chairman	President	Working President	General Secretary
Thiruvananthapuram	Ahmedabad	Kolkata	Chennai
M: 09447177456	M: 097277 60641	M: 0983081586	M: 09841089111

Dear Comrades, **21st October , 2016**

News of Interest 21st Oct

QUOTE OF THE DAY

"YOU HAVE TO LEARN THE RULES OF THE GAME. AND THEN YOU HAVE TO PLAY BETTER THAN ANYONE ELSE."

UNKNOWN

1. **DEBIT CARD SCARE: CHANGE ATM PIN IMMEDIATELY**

2. **GOVT ORDERS PROBE INTO DEBIT CARD DATA BREACH**

3. **HSBC TO WIND UP P-NOTE BUSINESS IN INDIA**

4. **BAJAJ AUTO TRADE UNIONS SAY HIKE IN WAGES NOT ENOUGH, THREATEN TO GO TO COURT**

5. **RBI RELAXES NORMS FOR FOREIGN INVESTMENT IN START UPS**

6. **YES BANK SEPTEMBER QUARTER PROFIT UP ABOUT 31 PER CENT**

7. **'NON-DISCLOSURE OF ATTACK COULD BE A VIOLATION'**

8. **RS 2,300 CRORE BLACK MONEY DETECTED BY DGCEI**

Business Standard

1. Debit card scare: Change ATM PIN immediately

With debit cards of 5 banks compromised, time to be very cautious while transacting. If possible, avoid non-bank ATMs

Priya Nair

Recently, many customers have got mails and messages from their banks to change the ATM PIN of their debit cards. We now know the reason, with reports suggesting 3.2 million accounts in five leading banks -- State Bank of India, Axis Bank, ICICI Bank, HDFC Bank and YES Bank -- are compromised.

Bankers and cyber experts advise that ideally an ATM PIN should be changed every three to six months. Are they being overly cautious? Perhaps not. Several banks have already asked their customers to change their card security details and to stick to own ATM networks.

According to Reshmi Khurana, country head-operations for Kroll Advisory Solutions, there are reports of customers reporting transactions on their debit cards in China, which is how banks came to know of the breach of data security. A certain foreign payment services company, whose system is believed to have been compromised, is going for a forensic audit. "While it is not confirmed, the breach of data seems to be on account of amalware inserted in a white-label ATM network, which is why banks are cautioning their customers to stick to their own bank's ATM network," she says.

An ATM breach means the PIN numbers of not only that bank's customers but all those who use that bank's ATM network could be compromised. For most customers, using the card at an ATM would seem a safe transaction, being monitored by the bank. However, not always so. About 70 per cent of ATMs in India are running on outdated Operating Systems (OS), making it easier for fraudsters to exploit.

"Microsoft withdrew all support to Windows XP about two years before. But, there are still many ATMs running on Windows XP OS, which makes them vulnerable to malware and fraud," points out Harshil Doshi, consultant at Force point, a data privacy and security company.

Most banks also use ATM machines of different vendors, due to which standardisation of networks and technology is not possible. This also opens the system to possible fraud, Doshi adds. Fraudsters have developed devices to infect all types of ATMs.

What can you do to keep your accounts secure?

- Keep a track of your debit card transactions for discrepancies. Transactions of small amounts, or at odd hours, or from an unknown place indicate misuse
- Sign up for SMS alerts for all ATM transactions to be aware of any fraudulent transaction immediately
- Change your PIN once in three months, or at least once a year
- Use different PIN numbers for different ATM cards so that if one gets compromised at least the others are safe
- Never disclose your PIN number to anyone. Phising calls may offer to renew your reward points
- Don't disclose your PIN number to the shop attendant while swiping your card, even if it is a store you visit regularly.

"Once the malware is detected, the bank or payment services company will fix it but the problem is to identify the malware. While such incidents are common overseas, they are increasingly happening in India, too, as banks adopt more technology and

transactions become digital. There is a need to be more pro-active and put the proper checks in place,'' Khurana adds.

Operating expenses on digital security have to go up manifold, says Piyush Singh, Director at Accenture India. "While we have leapfrogged in digital technology, we still lag in digital security. Both banks and customers need to actively protect themselves. Going ahead, customers may ask a bank about its digital security and protection before opening an account and not only about services and rates. For banks, it is a question of their reputation,'' he says.

2. Govt orders probe into debit card data breach

641 customers of 19 banks identified as victims so far; banks issue advisory to customers

Nupur Anand

Banks, National Payments Corporation of India (NPCI) and the government got into damage control mode on Thursday to curtail the risks emerging from a possible data breach of 3.2 million debit cards.

NPCI issued a statement quantifying the damage: "The complaints of fraudulent withdrawal are limited to cards of 19 banks and 641 customers. The total amount involved is Rs 1.3 crore as reported by various affected banks to NPCI."

In what is being termed as one of the biggest ATM security breach in India, debit cards of bank account holders with State Bank of India, ICICI Bank, HDFC Bank, YES Bank, Punjab National Bank and some others have been compromised.

NPCI said the problem was identified when there were complaints from a few banks that their customers' cards were being used fraudulently, mainly in China and the US, while the customers were in India. "Apprehending that this could be a case of card data compromise, all the ATMs/PoS terminals in India and three card networks — RuPay, Visa and MasterCard worked in a collaborative manner in September 2016," said NPCI in a statement.

Earlier during the day, banks accepted that there was a data fraud and issued advisories. The government immediately stepped in and has asked NPCI to probe how the data breach took place and submit a report with suggestions on preventive measures, said a senior finance ministry official.

A P Hota, MD & CEO, NPCI said, "Necessary corrective actions have already been taken and hence there is no reason for bank customers to panic. Advisory issued by NPCI to banks for re-cardification is more as a preventive exercise."

NPCI said it was working closely with all stakeholders and once the forensic investigation is over, it would issue a further set of recommendations as precautionary measures to member banks.

According to sources, the issue was also discussed at the Reserve Bank of India's board meeting in Kanpur on Thursday.

As a result of this data breach, banks issued advisories to their customers to change their personal identification number (PIN) and to immediately report in case they suspect any fraudulent transactions. Lenders explained that even in this time of interoperability, where customers are allowed to use other banks' ATMs, concerns arising from third-party players have increased.

Lenders such as SBI and ICICI Bank said the data breach did not take place at their

ATMs. ICICI Bank said, "As a precautionary measure, the PINs of debit cards used at the ATMs of that bank have been changed." SBI announced that it would re-issue 600,000 debit cards where it believes data could have been compromised.

"We have sent out an advisory to SBI to cancel the debit cards of those customers who have not changed their PIN despite being asked, and issue new debit cards to them free-of-cost. Besides, as far as other instructions are concerned, Indian Banks' Association is giving out guidance," said a senior official from the finance ministry's Department of Financial Services.

Kolkata-based UCO Bank has also said it will replace some of the debit cards. However, the number of such cards would be less than one per cent of the total debit cards issued by the bank, said a spokesperson.

"One of the processors of Hitachi Payments' central switch had been attacked and the malware deployed on its switch was active for six weeks. Data of all the transactions passed through the switch has been possibly compromised. This happened at YES Bank, White Label Operator ATM (WLA) and a Korean bank ATM," said a person involved in the investigation. It is believed that cards used at around 90 ATMs have been affected.

YES Bank, however, said it has not seen any data breach so far. "YES Bank has proactively undertaken a comprehensive review of its ATMs, and there is no evidence of a breach or compromise on YES Bank ATMs," said a spokesperson.

Hitachi Payment Services on Thursday claimed that an external audit on its ATM networks that it manages for banks has not seen any breach of its systems. "We had appointed an external audit agency certified by PCI in the first week of September to check the security of our systems for any breach/ compromise based on a few suspected transactions that were highlighted by banks for whom we manage their ATM networks," said Loney Antony, managing director, Hitachi Payment Services. "The interim report published by the audit agency in September does not suggest any breach/compromise in our systems. The final report is expected by mid-November. The banks and card schemes are updated with the progress of the audit," Antony added.

SISA, a payments security specialist, is conducting a forensic audit of the data breach and is expected to submit details to NPCI by the first week of November. The company declined to comment on the issue, citing client confidentiality.

However, the banking regulator has not said anything about the issue so far. In the last few months, RBI has stepped up focus on customer awareness and cyber security. The central bank had come out with a draft circular on limiting liability of customers in unauthorised electronic banking transactions.

A K Viswanathan, partner, Deloitte Touche Tohmatsu India said, "This is a wake-up call and lays down an imperative for banks to rethink their cyber strategy and adopt stringent cyber security practices in every aspect of their operations."

As per RBI data, there were about 697.22 million debit cards till July-end.

3. HSBC to wind up P-note business in India

HSBC is among the top five issuers of P-notes in India with a market share of more than 6 per cent at the end of last financial year

Pavan Burugula |

HSBC is planning to wind up participatory notes (P-notes) operations in India, as tightening of regulatory framework has made the business unviable. P-notes'

attractiveness has been on the wane following tightening of the regulations and the recent double tax avoidance agreement (DTAA) with Mauritius.

HSBC is among the top five issuers of P-notes, or offshore derivative instruments, in India with a market share of more than 6 per cent at the end of last financial year. According to sources, the bank had set up an internal committee to study the developments around P-notes. The committee has suggested that incomes from P-note operations would decline in the next five years as the new norms have resulted in escalation of costs and regulatory burden.

"It is a part of HSBC's global restructuring strategy to shut the business vertical, which doesn't offer much growth potential. The bank has evaluated all the possible options on the table, including selling the P-note business. The decision to shut operations is in the best interest of the bank," said a banker.

According to sources, the renegotiated DTAA with Mauritius has also impacted the P-notes business of HSBC, which is registered in Mauritius.

When asked, HSBC declined to comment on the issue.

Other P-note issuers are also revaluating their strategy due to the changed scenario. As per experts, all the major P-note issuers are losing their clients. On the other hand, registrations as foreign portfolio investors (FPIs) have seen a healthy increase. According to data from Securities and Exchanges Board of India (Sebi), there were 5,322 overseas funds registered as FPIs in July 2016, compared with 4,311 during the same period last year.

"Participatory notes are no longer the most attractive route for overseas funds. These days, P-note holders are opting for direct route as procedures for direct registrations have been simplified. Even in terms of disclosures, if these investors come to markets as category-I or category-II FPIs, they don't have to disclose the end beneficiary while in case of P-notes they are required to disclose the same," said Suresh Swamy, Partner, PwC.

Earlier this year, Sebi increased the Know Your Customer (KYC) requirements, issued curbs on transferability and prescribed more stringent reporting for P-notes issuers and holders. It also mandated issuers to follow domestic anti-money laundering laws (AML), instead of norms prevalent in the jurisdiction of the end beneficial owner.

As per the revised DTAA agreement, short-term capital gains would be charged on all the investments coming from Mauritius. The capital gains tax would be 15 per cent from April 2019. In order to facilitate smooth transition, government has proposed to tax the investments from Mauritius at 7.5 per cent until March 31, 2019.

Further, all the investments made prior to March 2017 would come under the "grandfathering" clause and would be exempt from paying any capital gains. Currently, the P-notes assets in the country are around Rs 2.1 lakh crore — 8.4 per cent of the total FPI assets. The share of P-notes in the overall FPI assets has been coming down due to tightening of disclosure related norms. In 2007, P-notes accounted for nearly half of the FPI assets.

Financial Express

4. Bajaj Auto trade unions say hike in wages not enough, threaten to go to court

In yet another wage dispute at Bajaj Auto, workers at the company's Chakan and Akurdi plants on Thursday rejected an offer to increase wages by R10,000-11,500 with the unions threatening to go to court, reports Geeta Nair in Pune.
By: Geeta Nair

In yet another wage dispute at, workers at the company's Chakan and Akurdi plants on Thursday rejected an offer to increase wages by R10,000-11,500 with the unions threatening to go to court, reports Geeta Nair in Pune. The motorcycle maker, however, went ahead with the wage hike after talks with the workers union, the Vishwa Kalyan Kamgaar Sanghatana, broke down. A total of 1,000 workers will receive the hike which is to be paid in three instalments in FY17, FY18 and FY19.

In late June 2013, workers at the Chakan unit had struck work over a dispute on wage revisions but the strike was called off by the union unconditionally after 49 days. The dispute ended with the workers signing an agreement which gave them a hike of between Ra 9,000 and Rs 10,000.

On Thursday, the company stated in a notice the October10 meeting between the workers union and Pradeep Shrivastava, executive director, Bajaj Auto, had failed, after with it decided to go ahead with the hike and make advance payments. A section of workers, the notice said, had approached the management after negotiations failed — and it appeared there would be no hike — urging it to protect them from financial stress.

The company said these workers had agreed to adjustments in these payments once the final agreement was signed.

Bajaj Auto and the union had signed a nine-year agreement in May 2010 under which wages were to be reviewed every three years. The new wage agreement for the 2016-19 period was due in April 2016. On October 2, around 1,000 workers from its Chakan and Akurdi plants went on a day-long hunger strike to protest the delay in the wage settlement and to ask for the reinstatement of eight workers.
VKKS president Dilip Pawar alleged the management had imposed the wage agreement unilaterally without negotiated with the workers and so this is not acceptable to them. "The company deposited money into the bank accounts of the workers through NEFT without talking to them," Pawar said.

Bajaj has offered workers with over nine years' experience a hike of Rs 11,500, of which Rs 7,000 will be paid in FY17, Rs 2,500 in FY18 and Rs 2,000 in FY19. For those with six to eight years' experience, the hike is Rs 10,500, of which Rs 6,500 will be paid in FY17, Rs 2,000 in FY18 and Rs 2,000 in FY19. A hike of Rs 10,000 was offered for workers with five years' and less service, of which Rs 6,000 will be paid in FY17, Rs 2,000 in FY18 and Rs 2,000 in FY19.

Around 60% of the hike would come in the form of basic pay, DA, PF and gratuity, while the remaining 40% of the hike would be as allowances.

5. RBI relaxes norms for foreign investment in startups

Foreign Venture Capital Investors (FVCIs) can invest in Indian startups without prior permission of the RBI, the central bank said today.

By: PTI

Foreign Venture Capital Investors (FVCIs) can invest in Indian start-ups without prior permission of the RBI, the central bank said today.

Sebi-registered FVCIs have also been permitted to invest in unlisted firms in sectors like biotechnology, nanotechnology and dairy without prior permission of the RBI.

They will not require any approval from Reserve Bank and "can invest in…equity or equity linked instrument or debt instrument issued by an Indian 'startup' irrespective of the sector in which the startup is engaged," it said.

The RBI said the extant regulatory provisions have been reviewed and amended in order to "further liberalise and rationalise the investment regime for FVCIs and to give a fillip to foreign investment in the start-ups".

As per the amendment, FVCIs will not require any approval from RBI and can invest in "equity or equity linked instrument or debt instrument" issued by an Indian company in certain sectors whose shares are not listed.

The sectors are biotechnology, IT related to hardware and software development, nanotechnology, seed research and development, research and development of new chemical entities in pharmaceutical sector, dairy, poultry, production of bio-fuels, hotel-cum-convention centres and infrastructure.

FVCIs can also open a foreign currency account and/or a rupee account for the purpose of making transactions.

Also, there will be no restriction on transfer of any security/instrument held by the FVCI to any person resident in or outside India.

6. Yes Bank September quarter profit up about 31 per cent

Sept-quarter net profit 8.02 billion rupees versus net profit of 6.10 billion rupees year ago

By: Reuters

* Sept-quarter net profit 8.02 billion rupees versus net profit of 6.10 billion rupees year ago
* Sept-quarter interest earned 40.94 billion rupees versus 33.77 billion rupees year ago
* Sept-quarter provisions 1.62 billion rupees versus 1.04 billion rupees year ago
* Sept-quarter gross NPA 0.83 percent versus 0.79 percent previous quarter
* Sept-quarter net NPA 0.29 percent versus 0.29 percent previous quarter
* Consensus forecast for Sept quarter net profit was 7.65 billion rupees
* Sept-quarter NIM 3.4 percent
* Says reiterated approval for raising of funds by QIP up to US $1 billion
* Says provision coverage ratio (PCR) stands at 64.8 pct as at Sept 30, 2016
* Says reiterated approval for raising of funds by issuance of debt securities within limit of 100 billion rupees
* Standard restructured advances as a proportion of gross advances at 0.46 percent as at Sept 30, 2016, down from 0.71 pct as at Sept.30, 2015

7. 'Non-disclosure of attack could be a violation'

RAGHAVENDRA RAO K

Non-disclosure by listed banks to stock exchanges about issues such as cyber attacks on their systems or their ATM networks being infected by malware could amount to violation of SEBI regulations on listing obligations and disclosure requirements, say experts.

"As per the SEBI Listing Regulations, a listed company has to ensure timely and accurate disclosure of all material events to stock exchanges. Specifically, in terms of Regulation 30 of the said Regulations, a listed company has to disclose to the stock exchanges all such material events as soon as reasonably possible and not later than 24 hours from the occurrence of event or later along with an explanation for delay," said Tejesh Chitlangi, Partner IC Legal.

Material event

"Any fraud/material wrong perpetuating on a mass scale with respect to a product of a listed company may qualify as a material event. A violation may lead to regulatory warning, imposition of fines or other penalties depending upon the gravity of non-compliance," he added.

According to Vidya Rajaram, Partner Grant Thornton India LLP, the level of attacks is a fairly serious issue. "Hackers usually go after targets that are critical in nature so that the impact is maximum as it affects movement of money in the economy," she said. "This being close to warfare it is very difficult to achieve prevention and could be state sponsored/ or a group of criminals. Technology and /law enforcement is usually behind the curve in catching these criminals, she added.

Consumers should be wary

Consumers should also take adequate safeguards while transacting online, says Mukul Shrivastava, Partner, Fraud Investigation & Dispute Services, EY India.

"While companies are doing their part, consumers can also take certain precautionary measures at an individual level to combat online fraud. For instance, they can avoid sharing any private factual information, especially on social networking sites, use unique passwords and change them at regular intervals to mitigate surging cases of identity thefts," he said. "We have seen that technology — though it can be a double-edged sword — can minimise cyber-attacks and security breaches to a large extent."

Rajaram sums up: "This is not a problem of technology but one related to humans. Companies need to constantly check their cyber resilience and readiness by doing mock drills/ ethical hacking instead of waiting for something like this to happen. On its part SEBI may enact a regulation which would require companies to disclose their cyber-readiness."

8. Rs 2,300 crore black money detected by DGCEI

The Directorate General of Central Excise Intelligence (DGCEI) has detected and seized massive records of black money to the tune of Rs 2,300 crore at a secret office of a Kanpur-based iron and steel products maker.

By: PTI

The Directorate General of Central Excise Intelligence (DGCEI) has detected and seized massive records of black money to the tune of Rs 2,300 crore at a secret office of a Kanpur-based iron and steel products maker.

Acting on intelligence, the DGCEI officials found that the private firm was allegedly evading excise duty in manufacturing of iron and other products.

The company was allegedly maintaining a secret office in Kanpur to keep a record of actual sales and evading payment of tax to the government by showing less sales, according to a press release issued today by the DGCEI.

"This (maintenance of secret office) was being done to avoid declaring actual purchase, manufacture and sale of iron and steel products to the various tax departments of the Central and state governments to escape the tax liabilities," it said.

The DGCEI officials visited the secret office of the firm, which has a number of companies and is a leading manufacturer of TMT bars (Saria), iron and steel flats, billets, wires, etc, and detected Rs 2,300 crore black money (which is the total amount of unaccounted sales proceeds), the release said.

The Managing Director of the firm was interrogated yesterday and put under arrest, it said.

Recently, DGCEI had detected eight illegal packing machines of pan masala and gutkha in Dabri village area of New Delhi and arrested two masterminds.

In this financial year so far, DGCEI has recovered over Rs 1,000 crore from tax evaders in its central excise and service tax investigations, the release said.

With kind regards,

Yours Comradely,

(N. GOVINDRAJULU)
GENERAL SECRETARY