SVC CO-OPERATIVE BANK LTD. (Multi-State Scheduled Bank)
ESTD.1906
(Formerly The Shamrao Vithal Co-op Bank Ltd.)

Frauds / Cybercrimes through investment / part time job / Ponzi scheme scams

Of late, Banks are witnessing the incidence of a number of cybercrimes wherein the criminals and fraudsters are resorting to different kinds of modus operandi for perpetrating cybercrimes routed through the banking channels and payment gateways. RBI, time and again, disseminates information about the frauds/cybercrimes and issue Advisories to the Regulated Entities (REs) which interalia include the course of actions to be followed by the REs. In this regard, we further advise the banks regarding such frauds and cybercrimes which have come to our notice in the recent past.

Some of the modus operandi followed by the fraudsters and criminals through investment / part time job / Ponzi schemes, wherein the transactions are routed through the banking channels are given hereunder:

1) Victims are lured through part-time job offers and other advertisements on Internet and/or messaging platforms, etc., and are promised high commissions or high returns such as doubling of money in short span of time. The advertisements / SMS messages usually contain a link, which directly prompts for a chat. Further, mobile applications, bulk SMS messages, SIM-box-based Virtual Private Network (VPNs) phishing websites, cloud services, virtual accounts in banks, Application Programming Interfaces (APIs), etc., are used to carry out financial frauds.

2) Keywords such as ‘Earn Online", "Part Time Job", etc., are used by fraudsters and criminals to match their advertisements with the terms people are searching for. Further, such advertisements are mostly displayed from 10 AM to 7 PM,which is usually the peak time for internet use by Indian public. Majority of websites used by fraudsters have domains - ’Xy2’ and ’wixsite'. Most of these sites either redirect to a messaging platform or to a website which has embedded messaging platform link which, on clicking, again redirects to a chat.

3) Multiple Indian numbers were used for communication with victims. Upon analysis, it was found that mobile number holder was not aware about messaging platform being operated in his/her name. In some cases, the mobile number holder knowingly shares OTP in return for some money from the fraudsters.

4) The fraudster sends an investment link over chat. Each person has a referralcode. Fraudster generally communicates in English. Google Translate is alsoused to communicate with the victims.

5) A screenshot needs to be sent to the person over the messaging platform to activate the account. Once the account is activated, a task is given to the user to gain confidence of the person. Mandatory condition to do a task is to load money through Payment Gateways which are not authorised to operate in India. All payments are made through digital channels including UPI. Some of the UPI addresses belong to companies registered with Ministry of Corporate Affairs (MCA). A call centre is usually used to interact with the victim for communication regarding tasks. For instance, on failure to load funds on investment website, the call centre executive initiates a call.

6) Once the task is completed, the victim is asked to withdraw the money. Money is withdrawn through various Payment Aggregators.

7) On getting the first refund, the victim is now lured to do more tasks which involve loading of more money. The process continues and once a big amount is loaded by the victim, the person (fraudster) stops responding over chat.

8) UPI details are updated daily on the fraudulent websites. Investment websites keep changing. Source code remains same but domain changes.

9) Bank accounts opened by money mules using real / fake identification are used to receive stolen funds from compromised bank accounts, through sharing of OTPs, etc. Rented accounts are sourced by agents and account owners (money mules) are given fixed rent or commission or lump sum amount for the account.

10) Layering of transactions is carried out by account to account transfers. Bulk payments / API's are also used for this.

11) From the intermediate account, money is diverted to multiple sources/assets like crypto currencies, bullion, payout accounts (for gaining confidence and hiding laundering), foreign money transfer, person-to-person transfer, etc.

12) Instances have been observed where Shell Companies with dummy directors, rented companies with MCA registration certificates, FinTech companies, payment gateways, SMS aggregators are reported to be involved in carrying out such financial frauds, mostly using UPI as payment mode. Main objectiveof opening Shell Companies is to create a current account or a FinTech company for accepting or paying out proceeds of frauds. Most of these Shell Companies appear to be Technology Companies created with 'Technology Private Limited' name and mostly registered with Bengaluru RoC.

13) UPI addresses are used to create layering behind Payment Aggregators thereby, facilitating end of day settlement.

14) Aggregator on aggregator concept is used by these players (fraudsters) in order to conceal their identities. The merchants' on boarded on the FinTech players (E.g. ABC Company on boarded on Payment Aggregator) are frauds. The network of fraudsters start creating Payment Aggregator business in collaboration with banks directly or with other FinTech companies. The fraudsters would be sittingbehind the payment aggregator as sub-aggregator or directly as a merchant.The money collected by the fraudsters, as sub-aggregator and/or as merchant, is remitted to the Payment Aggregator wherefrom the API (app) based payouts take place. After the aggregator network is set up, the accounts are operatedfor making the payouts by the fraudsters based outside India.

15) Accounting Professionals, foreign nationals (from Cambodia, China, Dubai, Nepal, Philippines, etc.), payment aggregators, points of sale terminals for SIM cards, etc., are also reported to be involved in such frauds.

16) Gold, crypto currencies, international money transfers are observed by Law Enforcement Agencies (LEAs) to be the usual termination points of the fraud trails.

Advisory to general public while using digital services

- Bank's esteemed customers are advised to refer contact information like Email address, Mobile number and Landline number of Bank officials, offices, branches always from Bank's official website i.e. svcbank.com only.
- Information available at various other places/ different websites may not be updated/ may contain misleading/wrong information and can divert/lead customers to become target of fraudulent activity.

Mobile Banking Security Advisory Alerts

- Verify the App Name and it's publisher before download
- Download the apps only from the Google Play Store and from App Store for iOS
- Verify the app permission and block unwanted permission
- Check and verify the App Notification for genuineness
- Install and Keep the Mobile Anti-Virus Up-to-date
- Keep the device and OS updated
- Be careful while browsing the Web sites through Mobile Browser and Ad's

Advisory to customers for Mobile Banking

- Secure your account, Register your mobile number & Receive transactional SMS alerts
- Beware of Phishing Attack! Phishing is a technique used by scamsters to illegally procure personal information, like Internet Banking User Id and Passwords, Debit Card Number and ATM PIN etc., by sending e-mail.
- The e-mail appears to be sent by Bank or a well-established organization providing online services. The content of the e-mail is framed in a manner that creates a sense of urgency in the mind of recipient, for example- "We are upgrading our system to make it more secure. Therefore, click on the link below and provide your Internet Banking User ID & Passwords at the earliest; otherwise your Internet Banking services will be de-activated." Customers of leading Banks throughout the world have been targeted by such Phishing e-mails.
- Never respond to emails asking for your Internet Banking Passwords.
- Never share your Account Number/Card Number/PIN/password/OTP with anyone over phone, SMS or e-mail. It may lead to fraud. Bank never asks for such information.
- Please register your Mobile Number with the Bank for SMS Alerts, if not done already.

- Please inform the Bank in writing immediately in case your Mobile Number registered for SMS alert is changed.
- Don't write the PIN Number on the Card or anywhere else. Please memorize the same.
- Please change your Pin/Password periodically for security reasons.
- Never share Card details, PIN, CVV, OTP etc. with anyone. Bank does not call for such information from any Customer. Therefore, no information should be shared on telephone also even if the person calling from other end introduces himself as Bank official.
- In case your Debit Card is non-functional for any reason, please contact the concerned branch for issuance of a new Card.
- Please do not leave your Mobile with others
- Please go through the transactional alerts sent by the Bank through SMS and take up immediately with your Branch in case of any discrepancy.
- Always keep your Debit Card safely in your possession.

For Mobile Banking Users:

DOs:

- Set up password of mobile phone and do not reveal password to anyone.
- Smart Phones with GPRS are vulnerable to virus, so install up-to-date antivirus software in user mobile phone.
- Download and run security updates and patches on user mobile browser. This helps in protection from known possible security problems.
- Install a firewall on mobile handset or enable the same if handset comes with a firewall.
- Remove the temporary files and the cache that were stored in the memory of the phone regularly, as that may contain any sensitive information such as account numbers.
- Clear the browsing history regularly.
- Type in the URL for mobile banking in the mobile browser, instead of clicking on any link. This will ensure access of the authentic website of the bank.
- Delete spam messages/mails.
- Be aware of the potential for fraudulent SMS messages. The Bank will never request or invite customers to logon to its mobile banking service via a SMS message.
- Check that the security padlock on internet browser is "locked" to ensure the connection is secure and protected by SSL. User should also check that the URL starts from `https` and not `http`.

- Avoid performing transactions or applications in public places. This helps in minimizing the risk of security threats such as "shoulder surfing" of mobile banking credentials.
- Keep mobile handset in an auto lock mode to provide additional protection.
- Monitor your account regularly and always keep a record of user transactions.
- While using Wi-Fi access, ensure that adequate security measures have been implemented on mobile handset to protect it against virus and attacks from other Wi-Fi users.
- Switch off the blue tooth function of handset when not in use. This protects from virus attacks.

DO NOTs:

- Do not share mobile banking credentials (user ID, passwords) with anyone.
- Do not share mobile handset with untrustworthy people, to restrict unauthorized access.
- Do not allow others to access your mobile phone before logging out from the sites (banking/financial/shopping) that you are accessing.
- Beware of online offers that require account details for `verification`. Do not reveal any information regarding account such passwords, account number etc.
- Do not leave Mobile banking application session unattended. Always sign off from a session.
- Do not follow any URL in messages that user is not sure about.
- Do not download any file from sites (e.g. applications, games, pictures, music etc.) or any e-mail attachments that you are not sure about.
- Do not download any software without verifying its security and privacy features from the website.
- Do not logon to the mobile banking application from a mobile handset that is shared with other people, as it may be difficult to ensure the handset is free of hacker or spyware.
- Do not save mobile banking credentials like user ID, passwords in the phone`s T9 dictionary. This helps to reduce the risk arising in case mobile phone is lost or stolen.

Advisory to customers while using Internet Banking Services

Online banking is safe and convenient as long as you take a number of simple precautions. Please make sure you follow the advice given below:

- Visit our Internet banking site directly. Avoid accessing the site through a link from another site or an e-mail and verify the domain name displayed to avoid spoof websites.
- Ignore any e-mail asking for your password or PIN and inform us of the same for us to investigate the same. Neither the police nor we will ever contact you to ask you to reveal your online banking or payment card PINs, or your password information.
- We advise you not to use cyber cafes /shared PCs to access our Internet banking site.
- We advise you to update your PC with latest anti-virus and spyware software regularly. You may install security programme to protect against hackers, virus attacks or malicious 'Trojan Horse' programme. A suitable firewall installed in a computer to protect your PC and its contents from outsiders on the Internet is recommended.
- Disable the 'File and Printing Sharing' feature on your operating system.
- Log off your PC when not in use.
- Do not store your ID/PIN in the Internet Explorer Browser.
- Check your account and transaction history regularly.
- Follow our advice - our websites are usually a good place to get help and guidance on how to stay safe online.

Advisory to customer while using ATM Card / Debit Card

- Always keep the card in your custody
- If you have lost your Debit Card, notify immediately by way of an SMS <STOPCARD> TO 9820620454 to hotlist user card, to avoid any misuse of card by anyone.
- Cancel any unwanted or expired cards by contacting the card-issuer and cutting up the unwanted or expired card in at least two pieces.
- It is recommended that mini-statements are regularly generated for reconciling/checking the transactions.

Suggestions while handling PIN

- While receiving the PIN please ensure that the envelope and the security document are not tampered with. In case of tampering contact the base branch immediately and do not use PIN.
- Do not keep the PIN along with the card. Always memorize the PIN and destroy the PIN mailer.
- Change ATM/ Debit card PIN through SVC ATM, immediately at first use.
- Change PIN number at frequent intervals or when it seems to have been compromised/ shared.
- Do not choose a PIN that can be obviously associated with user- e.g. telephone number, birthday, street number or popular sequence numbers (1111, 1234 etc.). Choose a random combination of number.
- Never write down or record user PIN or other security information on card or at a place easily accessible by others.
- Do not reveal user PIN or any security information on card to anyone. Neither the Bank nor any Authorized Agencies will ever ask you to disclose your PIN. In case of any such happening please note the particulars of the caller and report to the nearest branch for an appropriate action.

Precautions while using Cards for Point of Sale (POS)

- While making payment at POS always ensure that the card is swiped in your presence only
- Do not share PIN or any security information related details with anyone.
- Always check Debit card when returned after purchase.
- Insist for a copy of receipt and retain it till the account statement is checked.

Precautions while using Cards at ATMs

- Do not conduct any transaction on ATM, if you found the surroundings suspicious. Look out for suspicious devices on ATMs or pin pads.
- Do not accept help from strangers/guards and never allow yourself to be distracted
- Always ensure while doing transactions, no one is present around ATM machine.
- If there is anything unusual about the ATM machine, or there are signs of tampering of machine, do not use the ATM machine and report to Bank immediately.

- Use your body to block the view of user transaction. Especially while entering PIN and withdrawing the cash.

- Don`t discard receipts and mini-statements or balance inquiry slips which contain important information. User gets a receipt every time user makes an ATM transaction. Tear up or preferably shred the user cash machine receipt, mini-statement or balance enquiry when disposing them off.

- After completing transaction, remember to take your card back.

- If the ATM machine does not return the card, report its loss immediately to user Bank/branch on the numbers displayed in SVC ATMs.

Safety Measures While Using Internet/Debit Cards For Online Shopping/E-Commerce Transactions:

- Be sure of the website address before using the website for online shopping. Always type the website address into the address bar or bookmark the websites that are frequently used.

- Never enter, confirm or update net banking/card related details in a pop-up window.

- Shop only from secured and reputed websites- ensure that the security icon, the locked padlock or unbroken key symbol, is appearing in the bottom right of web browser window before sending your card details.

- Click on the security icon to ensure that the retailer has a valid encryption certificate – the address on this certificate should conform to the address on the address bar. The certificate should ensure the identity of the website and the current day`s date should be within the validity dates of the certificate.

- Users must not respond to online offers that require user`s account details "for verification".

- Users must be fully aware of any payment commitments that he is entering into, including instructions for a single payment or a series of payments

- It is advised to save the transaction receipts of utility payments on your hard disk which be printed as well. It can be referred to in case of mismatch with Internet transaction history or the already paid bill may reappear in next billing cycle.

- User should register for SMS alerts through ATM/Branch, for receiving alerts of specific transactions done through Internet banking/Debit card.

- The beginning of the retailer`s Internet address will change from `http` to `https` when a purchase is made using a secure connection.

- User must use trusted sites only, for example sites user know or that have been recommended to user or that carry the Trust logo.

- Avoid signing up for junk mail – this may result in pre-filled application forms being sent to an address long after user has moved out.

- If user has any doubts about giving user card details, find another method of payment.

- Keep passwords secret. Some online stores may require user to register with them via user name and password before buying. Online passwords, including, the one, verified by user issuer, should be kept secret from outside parties the same way user protect user Card PIN. Keep the login information safe and secret.

- Never send payment information via email. Information that travels over the Internet (such as email) is not fully protected from being read by outside parties. The most reputable merchant sites use encryption technologies that will protect user private data from being accessed by others as user conduct an online transaction.

- Never click on Hyperlinks within e-mails. If you are sure that the company is genuine then directly type in the URL in the internet browser address bar, or call the company on a contact number previously verified or known to be genuine.

- Don`t let websites or merchants store the card information. The exchange of encrypted transactions will be better than to allow the storage of identity information on data bases.