AU SMALL FINANCE BANK

Customer Education series

Contents

1. Safety tips while writing a Cheque

Do's - Writing a Cheque

- Date: Without a date your cheque will just not be cleared. Date is to be written in DDMMYY format. A cheque is valid for 3 months from the date mentioned on it.
- Do not leave spaces between words or numbers: When you write numbers and words in the cheque, be it Name or amount, never leave a space or gaps between them, because that gives a chance to add some alphabet or number and change the whole cheque.
- Make sure you cross the cheque saying "A/C Payee": If you are going to pay to some person and want to force that the payment should go to the same person bank account, in that case, you should be putting a double cross line on the left-top corner of cheque and write "A/C Payee" or "Account Payee", which ensures that the money will get credited only to a bank account and not be handed over to someone as cash over the counter.
- Add a line after the name and amount till the end: You should add a running line after the name and the amount in the cheque, which ensures that one can't add anything after the name and amount and misuse it.
- Cancel the word "Bearer": If you look at your cheque closely, in the "Pay" section, there is space for the name and then on the right corner it ends with "Or Bearer" , which means that either the person whose name is written in the cheque or anyone else who is bearing the cheque can encash it. So you should always cancel the word "Bearer" from the cheque, unless you really want it.
- Add a sign of "/-" after the amount": anyone can add more numbers at the end and increase the amount if there is enough space ahead of the amount written. To avoid the same you should add sign of "/- ".
- Figures = Words: The amount in figure must match the amount in words. Don't leave any blank space either in column of figure or on words' line. It is better to draw a line on the space left. While writing in words use the word "only" at the end.
- Signature: Only, and only, after filling all the above mentioned details, should you actually sign the cheque.

Don'ts - Writing a Cheque

- Not to Sign it Blank: The first and foremost thing which one should never do is signing a blank cheque. Signing a blank cheque could lead to zero solvency for the Bank account.
- Not to keep it in Improper Way: You should never fold, staple and pin the cheque.
- Not to write on MICR: Don't write or mark anything on MIRC code and cheque number otherwise clearing of cheque may not happen.
- Don't keep the Cheque unsafe: Never leave a cheque unsafe, especially if it is a signed cheque. On missing a cheque, contact your bank immediately. Stop payment on missing cheque would work as a safe custody for a missing cheque. Make sure impaired cheque is disposed of properly.
- Alteration/ Amendments: Don't make alterations and amendments on the cheque. Any alteration will result in rejection of cheque.

- Use a Pen: You should never use anything to write a cheque which can be erased. Always write clearly and avoid overwriting.

2. Safety tips to manage ATM cards

Do's – ATM

- Sign on the strip on the back of your card as soon as you receive it.
- Memorize your PIN (Personal Identification number) and destroy all physical evidence of the PIN.
- Always change the PIN as soon as you receive it.
- Register your mobile number with the bank for getting SMS alerts for your ATM transactions.
- Any unauthorized card transactions in the account, if observed, should be reported immediately to the Bank.
- Store your card in a secured place where you may immediately know if it is missing.
- Store the ATM-cum-Debit card carefully so that the magnetic strip does not get damaged.
- Beware of "Shoulder Surfing". Shield your PIN from onlookers by covering the keypad using your body while entering the PIN. If you want to cancel the transaction at any point of time, use the Cancel button in the ATM Terminal and before leaving the ATM
- Centre ensure that 'Welcome Screen' is displayed in the Screen.
- Contact The Branch In Case Cash Is Not Dispensed after account Gets Debited
- Please ensure that the card is swiped in your presence at POS (Point of Sale).
- If your ATM/ Debit Card is lost or stolen, immediately hot list the Card by informing the Bank.
- When you destroy your card upon expiry or closure of your account, cut it into four pieces through the magnetic strip.
- Look for extra devices attached to the ATMs. These may be put to capture your data. Inform security / bank immediately if any such device found

Don'ts – ATM

- Never lend your card to anyone, even to your close relative / friend or even if anyone claims to represent the Bank.
- Do not write your PIN on the Card or back of the Card.
- Never share your PIN with any one including a family member or Bank personnel or in response to requests through email.
- Never carry your PIN in your wallet or purse
- Never let anyone see you input your PIN
- Never use a PIN that could be guessed easily e.g. your birthday or telephone number.
- Never leave your card in the ATM
- Never leave your card unattended, e.g. in the car, in a hotel room or at work or at merchant establishments.
- Do not scratch the pin mailer. Tear the edge of the envelope turn to open for easy visibility of the pin

- Do not respond to any E-mail purported to have been issued by Bank asking for your ATM PIN. These are called PHISHING attempts. At AU SF Bank, we honor the trust reposed on us and will never seek personal details like PIN etc. for any purpose.
- Never enter your PIN in any ATM that does not seem to be genuine or seems modified/has a suspicious device attached/ operating in a suspicious manner.
- Don't display your cash; count the cash, keep it in your pocket safely and leave the ATM.
- Don't accept assistance from anyone or from the security guard when using an ATM
- Do Not Use Helmets, Cap etc. While Entering The ATM Room.

3. Safety tips for Mobile Banking

Do's – Mobile Banking

- Password protect the mobile phone. It is recommended to set the maximum number of incorrect password submissions not more than three
- Choose a strong password to keep your account and data safe
- Change your IPIN regularly
- Report a lost or stolen phone immediately to your service provider and law enforcement authorities

Don'ts – Mobile Banking

- Never give your PIN or confidential information over the phone or internet. Never share these details with anyone
- Don't transfer funds without due validation of the recipient, as funds once transferred cannot be reversed
- Don't store sensitive information such as credit card details, mobile banking password and user ID in a separate folder on your phone
- Don't forget to inform the bank of changes in your mobile number to ensure that SMS notifications are not sent to someone else
- Never reveal or write down PINs or retain any email or paper communication from the bank with regard to the PIN or password
- Be cautious while accepting offers such as caller tunes or dialer tunes or open/download emails or attachments from known or unknown sources
- Be cautious while using Bluetooth in public places, as someone may access your confidential data/information

4. Safety tips to manage Net Banking

- Your password should be complex and difficult for others to guess. Use letters, numbers and special characters [such as !,@, #,$, %, ^, &,* (,)] in your passwords.
- Do not use passwords that are obvious, like your name/nickname, names of your family members, your address, phone number, or any other information that a thief might find in your purse or wallet.
- Change your Internet Banking password regularly.

- If you have more than one Internet Banking user ID, use a different password for each of them.
- If you access any website (including AU SF Bank's website) from a cyber-cafe, any shared computer or a computer other than your own, change your passwords after such use in your own computer at your workplace or at home.
- Never share your passwords with others, including family members. Do not disclose your Internet
- Banking password to anybody, not even to an AU Small finance Bank employee.
- Let your password be a combination of character, number and special character.
- Do not write down or save internet banking password in notepads or personal devices.

5. Safety tips while Online Shopping

- Be very sure of the website address. The website address is reflected in the address bar of your Internet browser. This check is recommended every time you access any website from a link given elsewhere. Always type the website address into the address bar or bookmark the websites that you use frequently.
- Never enter, confirm or update your account-related details in a pop-up window.
- If you tend to use your credit cards for online shopping frequently, make sure that you sign up for the Verified by VISA Secure Code program(s).
- Confirm that the website is a secure one. Make sure any Internet purchase activity you engage in is secured by encryption to protect your account information. Look for "secure transaction" symbols.
- Shop only from reputed websites.
- Beware of online offers that require you to provide your account details "for verification".

6. General safety tips for Banking – Beware of Frauds

Phishing

- It is an attempt to 'fish' for your banking details. Phishing could be an e-mail that appears to be from a known institution like banks / a popular website. Please note that Banks will never ask for confidential data like login and transaction password, One Time Password (OTP), etc.

Spear Phishing

- Spear phishing is a targeted phishing attempt through an e-mail that appears to come not only from a trusted source, but often from someone in your own company, a superior in many cases, or from a close relative. The subject line address is customized / personalized and often will be one of relevance to either current projects of developments within the company, or may be related to family event. The violation occurs when the user opens the e-mails, clicks on the link attached and then Trojans or malware gets downloaded or a form appears on the screen, in which data needs to be filled in by the recipient.

Spoofing

- Website spoofing is the act of creating a website, as a hoax, with the intention of performing fraud. To make spoof sites seem legitimate, phishers use the names, logos, graphics and even code of the actual website. They can even fake the URL that appears in the address field at the top of your browser window and the Padlock icon that appears at the bottom right corner.

Vishing

- Vishing is an attempt of a fraudster to take confidential details from you over a phone call. Details like user id, login & transaction password, OTP (One time password), URN (Unique reregistration number), Card PIN, Grid card values, CVV or any personal parameters such as date of birth, mother's maiden name. Fraudsters claim to represent banks and attempt to trick customers into providing their personal and financial details over the phone.

Skimming

- Skimming is an act of stealing information through the magnetic strip on the cards that are used in ATMs and merchant establishments. Fraudsters collect information from a credit/debit/ATM card by reading the magnetic strip on the reverse of the card. For doing this, they conceal a small device in the card slot of ATM's or merchant payment terminals. This 'skimmer' scans the card details and stores its information. n tiny strategically positioned camera may also be used to capture the PIN. Skimming can occur in ATMs, restaurants, shops or other locations.

Smishing

- It is a combination of short message service (SMS - also known as text messaging) and phishing (the act of emailing someone with the intent of obtaining personal information that can be used for identity theft).Messages are being received across the country by cell phone users claiming their accounts are delinquent, need to be updated or even to register for a new program. Links in the message and toll-free telephone numbers are being used.

SIM Swap

- Under SIM swap/exchange, fraudster manages to gets a new SIM card issued for your registered mobile number through the mobile service provider. With the help of the new SIM card fraudster gets OTP & alerts required for doing financial transactions through your bank account

Other Safety Measures

- Never respond to unsolicited offers of money received through emails/phone/other media
- No one really gives you money for free
- Be careful while investing in seemingly attractive schemes offering high returns
- Don’t invest in unregulated companies/entities

- Don’t rely on hearsay - Check for yourself
- High return means higher risk including potential loss of entire money – Check your risk-appetite!
- Take care of your money – it is hard to earn but easy to lose
- When in doubt check with a trusted financial adviser