A Member Guide to Fraud Prevention

1. Protect Your Identity

Identity Fraud

Some key warning signs in recognising identity fraud include:

- You receive letters from solicitors or debt collectors for debts that aren't yours.
- You receive bills or invoices for goods or services you haven't ordered.
- You are refused a financial service (such as a credit card or a loan) despite having a good credit history.
- You are billed for a mobile phone contract (or similar) set up in your name without your knowledge

Always remember:

- Lock all valuable documents in a secure place.
- Shred unwanted documents and anything containing your personal or banking details (e.g. old utility bills, credit card receipts etc).
- Inform all service providers promptly when moving address.
- Protect mail left in communal areas of residential properties.
- Set up a mail forwarding arrangement with An Post/the Post Office.
- Never give your PIN number to anyone.
- Check your credit report with a credit reference service.

Bank and Credit Card Statements

Often times it is the early detection or notification of fraud that will assist or prevent further fraud.

- Regularly check your bank and credit card statements and bank transactions for evidence of fraudulent activity. Chase up any statements not delivered when expected.
- Report any suspicious or fraudulent activity to your bank immediately.
- Don't throw out old statements and/or receipts with your household rubbish. Dispose of it carefully, i.e. shred or burn it.

2. Stay Secure Online

Phishing

'Phishing' is a form of online fraud where fake emails or websites, supposedly from a legitimate company, seek to obtain your confidential account details. This is done with a view to conducting illegal transactions on your account.

If you think you may be a victim of a 'phishing' attack:

1. Notify the relevant financial institution.
2. Change your passwords.
3. Contact An Garda Síochána/Police

Always remember:

- Your bank will never send you an email requesting your bank security details.
- You will only need your security details when logging into your bank's internet banking service.
- Do not share your password with anyone.
- Do not open email attachments from people you don't know.
- Be wary of clicking on links, they can lead to false sites.
- Review credit card and bank statements regularly to reveal any problems and inconsistencies.

Online Security

'Spyware' is software that is downloaded onto your computer, without your knowledge. Once there it can steal a user's information or corrupt the user's system files and may transmit it to a third party.

Always remember:

- Install a reliable anti-spyware application.
- Ensure the application is kept up to date.
- Activate a firewall.
- Be security conscious when surfing and downloading.
- Only download from sites you trust.
- Read security information before you download software.

- Any unsolicited request for bank account information you receive through pop-up windows should be considered fraudulent and reported immediately.

Internet – Buying/selling online

When selling high-value goods and services over the internet be wary of cheques/drafts received for a sum in excess of the agreed amount. Fraudsters may claim that this extra money is to pay a handling agent or to cover shipping costs. Do not transfer funds from your own account in order to refund the 'surplus' money. Do not release high-value cash or goods until you are quite certain that the cheque or draft received by you has been paid. Bring such cheques or drafts to the attention of your bank before lodging. Report any fraudulent activity to your local Garda/Police station.

Advance fee fraud

The advance fee fraud occurs where people are persuaded to advance sums of money in the hope of gaining a much larger sum. Recent variations have seen claims by alleged members of staff of a bank who seek assistance to steal substantial sums of monies from dormant accounts. The information contained in the email is totally bogus; the sender is attempting to defraud the recipient. Do not respond to these emails. Avoid and report phishing emails and websites (e.g. support.google.com or satety.yahoo.com etc) to An Garda Síochána/Police.

Progressive Credit Union

3. Stay Secure Online

Security tips for your smartphone and tablet

- Lock – set your smartphone and tablet to automatically lock. A password protects your device so that no-one else can use or view your information. Store your device in a secure location.
- Contact your bank if you lose your smartphone or tablet – call your bank immediately to report the loss and provide your new mobile number especially if your bank uses an SMS message to authenticate transactions.
- Clear your mobile device of text messages from banks especially before sharing, discarding or selling your device.

- Be careful what you send via text – never use text messages to disclose any personal information, such as account numbers or passwords which could be used to steal your identity.
- Use only official apps – make sure to only use apps supplied by your financial institution and only download them from official app stores. Install apps from reputable app stores.
- Protect your tablet and smartphone – install and keep up-to-date anti-virus and firewall software purchased from trusted suppliers. It is important to update the software regularly to ensure that you are protected against new viruses.
- Protect your passwords – ensure you keep confidential your PIN and Internet banking logons and passwords. Avoid using the same login passwords for multiple websites, especially when it enables access to websites that include sensitive personal information. Set a passcode for your device and a PIN for your SIM. If your banking app allows login with a PIN, make sure it is different to the one used to unlock your mobile device. Make sure your password or code is something that's hard for others to guess but easy for you to remember.
- Read privacy policies – before you provide personal information to any website, understand how your information will be used and how long it will be retained.
- Be wary of free downloads, programs, software or screensavers – sometimes malware and spyware can be hidden in files offered free-of-charge.
- Beware hoax e-mails – be alert to offers that are 'too good to be true' or are designed to elicit an emotional response and triggers the thought of sending money. Always question messages that come out of the blue and verify the authenticity through trusted channels. Do not respond using information of links provided in the original message. No bank will ever send customers an e-mail with a link to online banking or ask for confidential information, so treat with suspicion any unsolicited e-mail that appears to be from your bank.
- Never reply to unsolicited texts – simply delete them.
- Check your bank account statements – contact your bank immediately if you find any unusual or suspicious transactions. Your bank will then take action to protect your account. Bank staff may call you before your statement has arrived to advise you of unusual activity on your account.
- Don't store your banking PINs or passwords in your smartphone or tablet – this makes your account vulnerable if the device is lost or stolen.
- Regularly clear your browser's cache – some mobile devices store copies of web pages that may contain your banking information.
- Always log out of internet banking sessions once you've finished.

- Be aware – when using internet banking in busy, public areas, check for people looking over your shoulder.
- Wi-Fi – don't conduct internet banking using unsecured public Wi-Fi networks or hotspots. Use a 3G or 4G data connection instead.
- Device security – Do not jailbreak your device and do not use jailbroken or rooted devices for internet banking. Jailbroken or rooted device is any electronic device not designed or authorised by phone manufacturers and network operators. Jail breaking your own device can significantly weaken its security.

4. Guard Your Cards

Card fraud

Chip and PIN has changed the way we pay for goods and services. It is easy and secure:

- Using your PIN to verify transactions will make card fraud considerably more difficult.
- Take care when entering your PIN – always keep it safe, cover the keypad when entering the PIN, never tell anyone what it is and never write it down or record it on any device.
- When paying for goods and services prevent cloning by insisting on being present when your card is being processed.
- You should never provide your PIN when carrying out telephone and internet transactions, or purchase by mail order.

Card fraud – holiday travel

When on holidays you will be more relaxed and perhaps less vigilant so here are a few tips:

- When paying for anything with your credit or debit card don't let the card out of your sight. You can always accompany the staff member to the payment terminal or ask if the terminal device can be brought to you.
- Consider whether it is necessary to carry all your cards with you when you go out. Leave unused cards safely locked away.
- Have details of who to contact (in your card issuing bank) in the event that you lose your card or it is stolen.
- Have your card number(s) and account number(s) details available in the event that you should lose or have your card stolen.
- Always keep your card(s) and data in a safe place.
- Be careful with your PIN, never divulge it to anyone for any reason.

ATM fraud

Golden rules to reduce ATM crime:

Always remember:

- Be aware of your physical surroundings.
- Check that other people in the queue are at a reasonable distance.
- Shield your PIN number with your hand to prevent hidden cameras or person from capturing your information. Never reveal your PIN to anyone.
- Use ATM machines which are in clear view and well lit. Be careful of machines in dark areas or places that don't appear to be well monitored. If suspicious, walk away.

Observe the ATM:

- Pay attention to the front of the machine: - if the front of the machine looks different from others in the area (for example, it has an extra mirror on the face), has sticky residue on it (potentially from a device attached to it) or extra signage, use a different machine and notify bank management with your concerns.
- Pay close attention to the slot where you insert your card, if you're visiting an unfamiliar ATM machine, examine it carefully for hidden devices. Even if you are familiar with an ATM machine, pay attention to any differences or unusual characteristics of the card reader.
- If the ATM appears to have anything stuck onto the card slot or keypad, do not use it. Cancel the transaction walk away and immediately notify your local Garda/Police station.
- Never try to remove suspicious devices.