

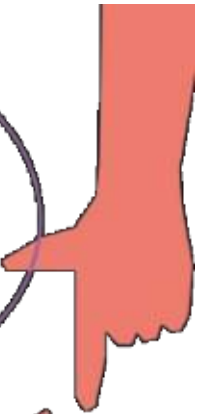


Protecting you and your Current Account from fraud





Pointing you in the right direction



How will I know if a call is genuine?

How do I keep my card details secure?

How do I shop online safely?

What should I do if I suspect fraud?





Fraud on Financial transactions is regularly reported in the News with Fraudsters becoming more sophisticated each day and producing frauds based on current topical news items. We need to do more to protect ourselves from becoming victims of fraud. While most financial frauds still use phone, texts and emails to commit the crime, fraudsters are using technology and publicly available information to trick people. As a valued member of our Credit Union, we hope this guide will help you to become more fraud aware. If you have any queries on this document, please contact your Credit Union.

Be Informed

- Stay in control, don't be rushed into making a decision you will regret.
- Don't assume you can trust the caller ID. Phone numbers can be changed so it looks like your Credit Union is calling.
- Fraudsters may already have basic information about you in their possession (e.g., name, address, date of birth) do not assume a caller is genuine because they have these details.

Be Alert

- To unexpected/unsolicited emails, telephone calls or texts. Always independently check the person is who they say they are.
- Always check your statements, and if you notice any unusual transactions, report them to your Credit Union or Credit Union Card Services immediately.

Be Secure

- Don't allow yourself to be rushed. Take your time to do the relevant checks.
- Never give your security details such as full online password, code/login details or PIN to anyone.
- Never use public Wi-Fi to make an online payment or access your online account, use your home or mobile data connection instead.





Card Safety – Keep your Card & PIN details Safe!

What to look out for:

- **ATM Distraction:** Be aware of others around you especially people offering help – If a stranger offers to help you at a cash machine, put your card away and leave. This is most likely a scam to try and see your PIN and steal your card.
- **Be Aware** of any damage or obvious fixtures to the ATM that look out of the ordinary. If in doubt, use another ATM.
- **Lost or Stolen Cards:** Fraudsters have been known to intercept Debit Cards and PIN numbers in the post. Be mindful of leaving post sitting in a mailbox especially if you live in an apartment block where other people may have access to the post boxes or if you are away for a period of time.

What you can do:

- **Shield** your PIN & check there is no one near you before using an ATM.
- **Don't** use the ATM if there are signs of tampering.
- If the ATM doesn't return your Debit Card, report it to your Credit Union or contact Credit Union Card Services immediately on **+353 1 693 3333 available 24/7**.
- **Protect Your PIN:** Your Debit Card is secured with a Chip & PIN – do not share your PIN with anyone.
- **Never write** your PIN down or share it with anyone. If you believe your Debit Card or PIN has been compromised, contact your Credit Union or Credit Union card services immediately on **+353 1 693 3333 available 24/7**.
- **Payment Terminals:** Never let your Debit Card out of your sight when you are making payments such as for a purchase in a retail outlet, restaurant, bar or parking machine. Insist that your Debit Card is visible to you at all times.
- **Report** your Debit Card as Lost or Stolen as soon as you have identified it as missing from your person or not received in the post after 10 working days to your Credit Union or Credit Union Card Services **+353 1 693 3333 available 24/7**.
- **Check** your receipts against your Credit Union statements regularly. If you find a transaction that you don't recognise, inform your Credit Union or Credit Union Card Services **+353 1 693 3333 available 24/7**.
- You should consider putting your Credit Union telephone number and Credit Union Card Services telephone number in your phone should you need to report your card as lost/stolen.



Protect your Passwords - Be Password Savvy!

- ❖ There are many simple ways for you to stay safe online.
- ❖ Using a strong password is a good way to start.
- ❖ If you use a password to log on to your network or computer, use a different password for orders or retailer accounts.
- ❖ Avoid using your address, birth date, phone number or easily recognisable words.
- ❖ The best passwords are alpha-numeric (using letters and numbers) and at least 8 characters in length.
- ❖ If you follow these simple steps, it will help to keep your Current Account Safe and Secure

What you can do:

- Use the security settings on your device - You should turn them on and set them to the highest level possible.
- Use a PIN or password - Set up a PIN or password on your device that only you know.
- Choose a strong password - Pick a password only you know and don't share it. Avoid using simple combinations such as "1234", "0000" or passwords that are easy to guess like "password123". Don't use words or numbers personal to you such as dates of birth.
- Don't let anyone else use your password - Keep your Online Account access safe, even if you have a joint account.
- Keep your security questions safe - If you have to set a security question, don't use personal information, and don't share it with anyone.
- Don't use the same password - Choose a new, strong password for every site you use.
- Don't write passwords down - Do not write passwords down. If you have to keep a reminder don't write them in full and keep them safe.

If you think someone else knows your personal account details contact your Credit Union or Credit Union Card Services on +353 1 693 3333 available 24/7





Shopping Online - Know who you are Dealing with!

Online fraud is the use of the internet to defraud or take financial advantage of you. Fraudsters do this by accessing your online Current Account or by presenting you with false offers in order to get you to transfer money or provide them with your Debit Card details. The internet is part of our daily lives for shopping, banking and connecting socially. While it brings many opportunities it also allows criminals attempt crimes from a distance reducing their chances of being caught.



What you can do:

- Exercise Caution when buying or selling items online by ensuring you are protecting your personal information.
- Research as much as you can about the retailer before you purchase anything from them. Use online stores that your friends and colleagues have used successfully or ones that you have heard about through trusted sources.
- Avoid deceptive websites when purchasing online. Copycat sites often pose as legitimate entities but are set up to take your personal information. Research the website and reviews via google, boards & social media.
- Never Disclose personal details such as account, online or PIN numbers in response to an email, phone call or letter claiming to be from your Credit Union. Financial institutions will NEVER request you to disclose your full passwords or PIN.
- Ensure that when you are shopping or making a payment online, that your internet access is secure
- The beginning of the website address should change from 'http' to 'https' before a purchase is made. This indicates that you are using a secure connection.



- Look for the Padlock!! Click on the security icon (the padlock or unbroken key symbol) to ensure that the retailer has an encryption certificate. The link should describe the type of security and encryption being used. If in doubt do some further independent research before using the website.
- Don't use unsecured public Wi-Fi networks or hotspots to make a card purchase or access your online account. Use your home or mobile data internet connection instead.
- Do not click on links or pop-ups or ads that state that you have won a prize

Always check your statements and report unusual activity to your Credit Union or Credit Union Card Services on +353 1 693 3333 available 24/7



Advertising Scams– Be Cautious!

Criminals can use false ads to trick you into transferring money, giving them your card details or other financial information. These false ads appear in many different ways including being sent to you by email or post, placed in a newspaper or public space or pop up while you are browsing online or on your social network feed.

What you can do:

- **Don't be Fooled** by ads on Social Media with 'incredible' offers. Research the company advertising the offer and remember – if it looks too good to be true, it probably is!!
- **Advance Fee Emails** intended to appear as a genuine business proposal, offering large sums of money in return for help. Do not open or action these emails. Report this immediately to your email provider and delete the email.
- **If Paying via PayPal** – When you are buying items online, select 'goods & services' at the checkout and not 'friends and family'.
- **Keep a record of your purchase** – Print out or save a copy of your order should you need to dispute the transaction in the future with the Merchant or your Credit Union.
- **Be Aware** of and do not respond to requests to purchase gift cards and then provide the code as a form of payment.
- **Always Read** the Terms and Conditions before you sign up to any agreement or purchase goods /items taking particular care where you might be signing up to a continuous authority agreement or subscription.

If you believe you have been a victim of Debit Card or any other type of financial fraud on your Current Account, report it immediately to your Credit Union or Credit Union Card Services on +353 1 693 3333 available 24/7.





Money Mules – Be Careful!

A money mule is a person who transfers illegally obtained money between different payment accounts, very often in different countries, on behalf of others. Money mules are also recruited by criminals to receive money into their bank account, in order to withdraw the money and in most cases wire it overseas, receiving a commission payment in return for the provided services.

Even if money mules are not involved in the crimes which generate the money (cybercrime, payment and on-line fraud, drugs and human trafficking, etc.), they are acting illegally by laundering the proceeds of crime, helping criminal syndicates move funds easily around the world and remain anonymous. If you are caught acting as a money mule, even if done so unwittingly, you can face a prison sentence, fine or community service, and the prospect of never again being able to secure a mortgage or open a bank account.

HOW ARE MONEY MULES RECRUITED

As new technologies and trends emerge; organised crime groups develop new systems to defraud people:

- seemingly legitimate job adverts (e.g.: ‘money transfer agents’)
- seemingly legitimate online posts
- direct approach in person or through email
- social media (i.e., Facebook posts on closed groups)
- messages sent through instant messaging apps (e.g.: WhatsApp, Viber)
- Newcomers to the country (often targeted soon after arrival) as well as the unemployed, students and people in economic distress are the most susceptible to the crime.
- Men are more likely than women to be targeted to become a mule, as are those aged 18-34 years compared to people aged 55+.

WHAT TO DO? If you have received e-mails of this type do not respond to them and do not click on any links they contain. Inform the Gardaí instead.

If after reading this flyer you believe that you are participating in a money mule scheme, stop transferring money immediately and notify your bank, the service you used to conduct the transaction, and law enforcement.



Scam Calls: STOP and THINK – is this call genuine?

Fraudsters can phone people and pretend to be from your Credit Union, the Gardai, or other well-known companies. Scam calls can sound real and professional and are often combined with Phishing attempts. People can be pressured into disclosing their personal credentials through several means.

What is Phishing? - (Normally electronic means such as email)

A Fraudulent attempt to obtain sensitive information such as usernames, passwords and Debit Card details by disguising oneself as a trustworthy representative of a company or organisation in an electronic communication

Types of Fraudulent Calls:

What is Vishing? – (Voice and Phishing)

A fraudster can phone you, claiming to be from your Credit Union, bank, the Gardaí, Revenue or a service provider such as a telephone company, internet provider or computer company. They trick you into believing they are a legitimate representative of the organisation and that it is in your interest to give the information they ask for such as your personal financial credentials such as one time passcodes required for 3D secure transactions and setting up your smart phone with Apple Pay, Google Pay and Fitbit pay.

What is Smishing? (a combination of the words SMS (text message) and Phishing)

Text messages sent to random phone numbers requesting you to click on an attached 'link' to 'update' 'verify' or 'activate' your personal details on your account. The link brings you to a fake website where the fraudster is pretending to be the legitimate company.

What to look out for:

Unsolicited Phone Calls: Never divulge personal information including account details, Debit Card Number one time passcode (OTP) or PIN, online information over the phone. Verify the name and company of the person that has called you and if you are unsure of the caller hang up the phone and use other sources such as the utility providers bill, or search engines or professional networking sites on the internet to research the organisation or individual. Remember it is unlikely that your Credit Union will make an unsolicited call to you, and if they do, they will not seek your account details as they will have these to hand.



Don't Respond to high pressure tactics to divulge your current account or personal details if you are unsure of the caller, take their details and say you will ring them back. Independently verify the phone number they give you to ring back before returning the call.

A need to transfer money - Scam calls can try to get you to transfer money for security purposes or to a safe/secure/holding account. Do not do this. Your Credit Union would never ask you to move money to a 'safe' account.

Refunds - If a call offers you an unsolicited refund it may be a scam. Your Credit Union would never call you about a refund of any kind requesting your account details.

Test transactions - If a call asks you to do a test transaction, then it's a scam. Your Credit Union would never ask you to do this.

Calls from the Gardai - It's very rare for the Gardai to contact you regarding financial services. If they do call, tell them you will phone them back. Verify the Garda Station details you are to ring back before returning the call.

You're asked to log on to your computer - A scam call may tell you there's something wrong with your computer or ask you to download something to improve your computers speed or performance. They could pretend to be from your broadband provider or trusted software company. If you didn't ask for this call, it is most likely a scam, and you should hang up.

What you can do if you get a call from someone you don't know or are suspicious of

- **Never** divulge personal information until you have validated that the caller is a genuine representative of the organisation they claim to represent.
- **Advise** the caller that you will call them back once you have validated their identity.
- Look up the organisation's phone number (by using the phone book or their website) and make contact directly with them to validate.
- Do not validate the caller using the phone number they have given you (this could be a fake number).
- If the caller is genuine, they will understand and welcome your need to validate them.
- Fraudsters may already have basic information about you in their possession (e.g., name, address, dob, account details), **DO NOT ASSUME** a caller is genuine because they have these details.



●**Remember!** It takes two people to terminate a landline phone call, you can use a different phone line to independently check the caller's identity.

What is Spoofing?

Spoofing is the act of disguising a communication from an unknown source as being from a known, trusted source. Spoofing can apply to emails, phone calls, and websites. Spoofing Fraud is a common technique used by fraudsters in an attempt to obtain your personal and card information for the purpose of identity theft or financial gain. The fraudsters send text or email messages that appear to come from your bank or from legitimate businesses in an attempt to fool you into supplying your banking details. These text messages can appear within a genuine thread of messages and will request you to log in to a fake website or to call a number.

What is Investment fraud?

Investment Fraud is a method where scammers convince you to invest in a scheme, shares or commodities, that don't exist, or aren't worth the money paid for them. This scam is usually perpetrated through pressurised sales tactics. Scammers will target anyone who responds to them and build trusting relationships with their victims over a period of time. Unfortunately, many of these scams are successful. There are many types of scams fraudsters use to persuade you to part with your money.

If somebody contacts you out of the blue by phone offering you the opportunity to invest in shares that are about to go through the roof - hang up immediately. Do not respond to unexpected emails or click on adverts across social media or online. The criminals may have researched you and appear to know a lot about you. These criminals will do their homework and make it their business to know as much about you as possible before they contact you. They will give you details that you think only a genuine investment company would know, such as a previous investment or share information. Watch out for offers endorsed by celebrities, these endorsements are totally false. Be cautious where the rate of return is very high and often advertised as guaranteed or risk-free.

These criminals will attempt to build a relationship over time. And watch out! An initial small investment may actually produce some returns before you are encouraged to invest a larger amount. If you are contacted by someone claiming to be from a well-known company, check them out independently





with the company, look up the company on Google and ring the contact details on the website, not the number you have been given by the caller.

The caller may ask you to download software to your PC which will provide them unlimited access along with the ability take control of your PC and manipulate the images you are being shown on screen. They will say they are helping you to make a payment and will ask for login information to your online banking. Others will request payments to be made via Debit card. Never provide one time pass codes received via SMS. Never provide login or card information on foot of a phone call. Some of the scams ask you to buy Bitcoin or a cryptocurrency to invest in the scheme. They will set up accounts for you within these companies. Do not provide photo ID, Proof of address without verifying the legitimacy of the caller.

Remember: If it sounds too good to be true, it certainly is!

Cryptocurrency Scams

Cryptocurrencies like Bitcoin are popular investments. Like everything popular, they attract scams.

Fraud in cryptocurrency investment is on the rise.

What to look out for:

Someone calls who:

- Seems to know about you (they use social media)
- Promises big returns and offering to help you get them,
- Calls or emails unexpectedly with a sense of urgency

It's a scam. End the call. Don't trust; don't invest.

Your Credit Union or the Gardaí will never ask for the following:

- Your Debit Card PIN number or full online access details
- Request you withdraw money to hand over to them or transfer money to another account, even if they say it is in your name.
- To come to your home to collect your cash or Debit Card.

REMEMBER: If you're not sure about a call hang up the phone and report it immediately to your Credit Union or Credit Union Card Services on +353 1 693 3333 available 24/7

What to do if you are a victim of fraud?

If you suspect you have been the victim of fraud or have noticed unusual activity on your account, contact your Credit Union or Credit Union Card Services immediately and also report to your local Garda Station. Fraudsters move fast; the quicker you contact your Credit Union to safeguard your accounts the better.

For more Information contact your Credit Union or visit www.currentaccount.ie



Issued by Credit Union Card Services

Telephone +353 1 693 3333

Credit Unions in Ireland are regulated by the Central Bank of Ireland. MasterCard is a registered trademark and the circles design is a trademark of MasterCard International Incorporated. The MasterCard Debit Card is issued by Transact Payments Malta Limited pursuant to licence by MasterCard International.