This only applies if you have selected a Payment Facility

Q: What is online fraud?
A: Online fraud is any type of fraudulent activity that uses the internet. This includes scams designed to steal your money, personal information, or both, through websites, emails, social media, and other online platforms.

Q: What is payment fraud?
A: Payment fraud is a serious issue that affects individuals and businesses alike. It involves any type of fraudulent or illegal activity where someone uses stolen or fake payment information to obtain goods, services, or money.

Q: What is APP fraud and how do I avoid it?
A: APP (Authorised Push Payment) fraud is when criminals trick you into voluntarily sending money to their account by pretending to be a legitimate person or organisation. To avoid it:

• Verify the recipient's details before sending money.
• Be wary of urgent requests for money.
• Don't be pressured into making a payment.
• If a deal seems too good to be true, it likely is a scam.
• If you are asked to send money to a new account, that you have not sent money to before, verify that account before sending funds.

Q: What are the most common types of payment fraud?
A: Common types include:

• Phishing: Fraudulent emails, texts, or calls tricking you into revealing personal or financial information.
• Skimming: Criminals illegally copying card data at ATMs or point-of-sale terminals.
• Account Takeover: Criminals gaining access to your online banking or e-money account.
• Malware: Malicious software that steals your data.
• Authorised Push Payment (APP) Fraud: Tricking you into sending money to a criminal.

Q: What are the most common types of scams?
A: Most common types include:

• Romance scams. The fraudster preys on the victim's need for affection by establishing an online romantic relationship through social media or dating platforms, to later persuade them to send money to the fraudster.
• Investment scams: The scammer sets up a fake investment website promising easy and high returns with little or no risk. When the victim deposits the money, it becomes clear that such a return never existed.
• Advance fee scams: The fraudster sends an email or letter to the victim stating that there is a large sum of money, for example that the victim has won a lottery or an inheritance, but there are some fees that must be paid before the large sum is released.

• CEO scams: The fraudster poses as the victim's boss or senior manager and convinces them to make an urgent payment or change payment details for a contract or supplier. The fraudster gains access to the company's business email account through hacking or spoofing.

• Mule accounts: In this case, the fraudster convinces genuine individuals to act as 'money mules' for him, most often by paying the victim a portion of the fraudulently obtained funds. The 'mules' may be duped or willing to accept payments into their own e-money accounts from (unknown to them) stolen cards/accounts. They are then instructed to transfer the funds to an account under the fraudster's control.
• Gift card scams: gift cards are similar to cash and scammers exploit this by contacting victims with urgent situations, instructing them to purchase gift cards from specific stores, and providing the card numbers and PINs to access the loaded money, resulting in permanent loss of money for the victim.
• Deepfake: voice fraud is a relatively new method of attack but one that has proven highly effective. As the name suggests, a criminal fakes the voice of somebody else with software that can successfully copy his/her voice via a small audio sample.
• Employment scams: Scammers target job seekers, offering fake employment opportunities or requiring payment for job applications, pre-employment checks, or training.

Q: How can I protect myself from fraud?
A: Key measures include:

• Never share your PIN, passwords, card details, or CVV/CVC code.
• Never share personal documents like passports, national IDs, driving licenses.
• Be cautious of unsolicited emails, texts, or calls asking for personal information.
• Use strong, unique passwords for all your online accounts.
• Regularly check your account statements.
• Keep your devices operating systems, antivirus and anti-malware software up to date.
• Be wary of suspicious websites and online offers.
• Be cautious about online stores where you use your card details. Do some research online before completing your purchase to make sure the website or app is legitimate.
• Enable two-factor authentication (2FA) wherever possible.
• Only use trusted Wi-Fi networks when using your accounts or making purchases.
• Be very sceptical of anyone asking you to transfer money urgently.

Q: What is contactless card fraud, and how can I prevent it?
A: Contactless card fraud occurs when criminals use stolen cards or devices to make small, unauthorized contactless payments. To prevent it:

• Regularly check your statements for unauthorized transactions.
• Consider setting a limit on contactless payments.
• Keep your card safe and secure.
• If your card is lost or stolen, report it immediately.

Q: What is phishing?
A: Phishing involves criminals sending fraudulent messages that appear to be from your payment services provider. These messages often ask for your login credentials, card credentials, personal information, or to click on malicious links.

Q: What is two-Factor Authentication (2FA)?
A: 2FA gives you twice the protection over your emails and social media accounts, which are common entry points that fraudsters try to exploit to get access to your e-money accounts and cards. So even if cyber criminals have gained access to your password, they can't access your email or social media account if they don't have access to the second factor. For example, getting a code sent to your mobile phone when you sign in using a new device or change settings such as your password. This control will not trigger every time you check your email or social media account.

Q: What should I do if I suspect fraud on my account?
A:
• Immediately contact us.
• Change your passwords and PINs.
• Report the incident to the police or relevant authorities.
• Keep a record of all communication and actions taken.

Q: What should I do if my card is lost or stolen?
A:
• Immediately report the loss or theft to us.
• Request a new card.
• Check your account for any unauthorized transactions.

Q: What should I do if I am a victim of fraud or cybercrime?
A: For card and account holders living in England, Wales and Northern Ireland who have been a victim of fraud or cybercrime, report it at www.actionfraud.police.uk or by calling 0300 123 2040. In Scotland, victims of fraud and cybercrime should report to Police Scotland on 101.

In Malta, customers can report fraud to the Cyber Crime Unit, Malta Police Force, telephone no. +356 2294 2231, or email: computer.crime@gov.mt

Q: Where can I find more information about fraud prevention?
A:
• Europol's website - Payment Fraud | Europol
• Stop Scams UK - Home - Stop Scams UK
• Action Fraud - Action Fraud
• The UK International Consumer Centre - Common Scams | UKICC - The UK International Consumer Centre
• Crime Prevention – Malta Police - Crime Prevention | The Malta Police Force
• The European Banking Authority (EBA) website - Frauds and scams | European Banking Authority
• National consumer protection agencies.