Fraud Awareness Statement

At Glo Currency, we are committed to supporting and helping consumers that may have become victims of fraud. Below is a list of common fraud scenarios you may face, there may be other scenarios you come across as consumer fraud is always evolving. The best way to protect yourself against becoming a victim of a scam is by educating yourself on how the fraud works. Please review the below scenarios and ensure you never send money if you come across such a scenario or come across any similar situation.

Advance Fee Fraud

Advance fee fraud, also called upfront fee fraud, is any scam that, in exchange for a fee which can be requested through a money transfer:

-Promises to send you money, products, or services;

-Offers you the opportunity to participate in a special deal;

- Asks for your assistance in removing funds from a country in political turmoil; or asks for your assistance to help law enforcement catch thieves.

Whatever the scammers call the upfront fees (membership fee, participation fee, administrative or handling fee, taxes) all have one thing in common: the victims never see their money, or the scammers, again. Advance fee schemes come in many forms.

As is the case with all of the scenarios given here, never send money to someone you have not met, never send money in advance for a credit card or loan and do not use a money transfer service to pay for goods and services.

Debt Elimination Fraud

Unlike legitimate companies who work with debtors to help them responsibly repay their debts, debt elimination scammers promise to make you debt free in exchange for a modest upfront or membership fee (which can be requested by sending a money transfer) which they simply pocket. Victims pulled in by these schemes will certainly lose that fee, but they may also lose property, incur additional debt, damage their credit rating, risk identity theft, or face legal action.

If you receive a call with a promise to help with debt, hang up the phone, do not engage these fraudsters. Never send a money transfer if asked to do so to pay for a fee.

Phishing

Fraudsters are always looking for ways to get your personal or financial information. When they use the Internet to do that, it's called phishing. These scam artists send email or pop-up messages that might alert you to a problem with your account or state that you have a refund waiting. Some of these messages appear to come from legitimate companies.

Do not respond to or open any such messages. Always use a strong password on your email and social media accounts. Never give control of your pc to anyone. If you suspect that a virus or malware has been installed on your pc, contact a professional.

Identity theft

Identity theft occurs when criminals access enough personal information about an individual to commit fraud. They use various techniques to steal these details, from outright theft and social engineering to harvesting data through cybercrime. With this information, criminals can impersonate the victim in order to access bank accounts, fraudulently claim benefits or obtain genuine documents in the victim's name. Criminals are increasingly stealing identity data online, for example persuading individuals to disclose personal details and passwords through 'phishing' emails, and then trading the data.

Always use a strong password on your email and social media accounts. Never give control of your pc to anyone. If you suspect that a virus or malware has been installed on your pc, contact a professional. Do not engage with the fraudster and do not send money using a money transfer service.

Lottery & Unexpected Prize Scam

Lottery, sweepstake or prize draw fraud happens after fraudsters contact you to tell you you've won a large sum of money in an international lottery, sweepstake or other prize draw, or that you have won a prize such as a holiday or laptop.

The fraudster will contact the victim via mail, telephone, email, text message. A fee is requested by the scammer to release the funds/prize. They will often claim that the fees are for insurance costs, government taxes, bank fees or courier charges. The scammers make money by continually collecting these fees and stalling the payment of winnings. In order to avoid victims from

further looking in to this or asking someone about the scam, fraudsters will urge the victim to keep the information confidential and to respond quickly.

Never provide your personal information in such a scenario, ask yourself how can you have won a lottery if you have never bought the lottery?, Do not send money to someone you have not met.

Romance Scams

Romance scams involve people being duped into sending money to criminals who go to great lengths to gain their trust and convince them that they are in a genuine relationship. They use language to manipulate, persuade and exploit so that requests for money do not raise alarm bells. These requests might be highly emotive, such as criminals claiming they need money for emergency medical care, or to pay for transport costs to visit the victim if they are overseas. Scammers will often build a relationship with their victims over time.

Common signs to look out for: the relationship progresses too quickly, the other person is not willing to meet, the other person wishes to communicate through personal email and not through a dating site, the other person claims to be in the military, the photos sent look too good to be true, the other person is based in another country, requests to send money through a money transfer for an emergency or to visit which never materialise. Do not send money to someone you have not met.

Rental Fraud

Rental fraud happens when would-be tenants are tricked into paying an upfront fee to rent a property. In reality, the property does not exist, has already been rented out, or has been rented to multiple victims at the same time. The victim loses the upfront fee they have paid and is not able to rent the property they thought they had secured with the payment. Rental fraudsters often target students looking for university accommodation. Rental fraud is a type of advance fee fraud.

Ask yourself, does the property appear to be too good in relation to the price being asked? The scammer will usually claim to be in another country and will ask for a deposit to be sent via a money transfer company. Do not send money to someone you have not met.

Emergency Scam

Emergency scams usually target parents, grandparents or other family members. Someone calls or sends a message claiming to be a child or grandchild in trouble or the friend of a family member who is in trouble and urges the victim to wire or send money immediately to help with an emergency. The caller will often claim to be embarrassed by what has happened and will ask the victim to keep the assistance secret from other family members.

Always call or text the family member having the issue to check if they are really in trouble. Do not be pressurised by the scammer. The scammer may hand the phone to what the scammer claims is the police, this may all be part of the act.

Grandparent Scam

Grandparent scams (also called grandchild scams) are common scams that target seniors and is a type of emergency scam. These scams usually involve a phone call or email from someone who pretends to be your grandchild. Acting as your grandchild, the scammer claims to be in trouble and asks for your help. The scammer may try to convince you that your grandchild was in a car accident or has been arrested. You may be asked to wire money or send money right away, without telling anyone.

Always call or text the grand-child having the issue to check if they are really in trouble. Do not be pressurised by the scammer. The scammer may hand the phone to what the scammer claims is the police, this may all be part of the act.

Anti-Virus Company Fraud

There are different variants of this scam. One type is Internet users could be targeted by fake call centres and pop-up adverts tricking them into downloading and paying for fake anti-virus (AV) protection, which is actually malicious software. Another type is where tech support scammers are pretending to be from Microsoft, McAfee, and Norton to target users with fake antivirus billing renewals in a large-scale email campaign. Another variant is being contacted by a re-known company that claims that there is a virus on your pc which they need to remove for which there is a small fee. In reality, there is no virus on the PC.

Do not give any details to anyone claiming to be calling from a company and is looking to help you. Do not let them access your PC. If you receive an email, delete the email and do not click on any links in the email.

Recruitment Scam

Employment fraud happens when a fraudster claims to be a recruitment agent, hiring you for a job – which can be in a foreign country - that doesn't exist. You place your CV or personal details on internet job sites so that potential employers can see them and, hopefully, offer you a job. Once you have received the job offer, they agency will tell you that there are various fees that you have to pay which can include admin fees, deposit on accommodation etc. Bank account details may also be requested for salary payments but they are instead used to steal money from the account. In reality, there is no job and any fees paid go straight to the fraudsters.

Fraudulent cheques may also be sent which will bounce when banked, this is explained in more detail in the next section.

Ask yourself, is the offer too good to be true? Do not send money to someone you have not met. Do not send money for a cheque deposited in your account, this can take weeks to clear.

Fraudulent Cheque Scam & Overpayment Cheque Scam

As part of a scam, victims are frequently issued a cheque and instructed to deposit it and utilise the cash for various expenses (cheque could have been sent for services provided). The cheque is a forgery (counterfeit), and the victim is liable for any monies spent with it. A deposited cheque can take several weeks to clear and funds from it should not be used until this time period has passed. The cheque may also be for a service or for a product with the amount greater than what is required, the fraudster will request for the cheque to be banked with the access sent back to the fraudster. By the time the bank has identified the cheque as fraudulent, the victim would have already sent the money and the victim would be liable to the bank for the funds. This is also linked to the next type of fraud.

Mystery Shopper Scams

The victim is contacted via an employment website, or the victim answers to an advertisement for a job opportunity to review a money transfer service. The fraudster frequently sends the victim a check to deposit and advises them to

send a money transfer, keeping a portion of the check as payment. The victim pays the money, the fraudster receives it, and when the check bounces, the victim is held liable for the entire sum.

Charity Scam

This refers to requests for charity for a charity that is non-existent. The request can be made via email or over the phone and the request will be made to use a money transfer company to send the money. Genuine charities do not request money to be sent using a money transfer company.

Tax Scam

The victim is contacted by a fraudster claiming to be a government official and demands immediate payment for outstanding taxes. A government official would never contact you to demand payment, demands for taxes are always made in writing.

Extortion and Sextortion

Scammers use threats of death, arrest, or other forms of coercion to get money, property, or services from a victim that they allegedly owe and threaten them if they do not agree. Sextortion scams are a type of phishing attack whereby people are coerced to pay a ransom because they have been threatened with sharing video of themselves visiting adult websites.

Visa & Immigration Scams

Immigration fraud is generally defined as individuals and companies who target vulnerable immigrants by providing unauthorized and fraudulent immigration services. The victim could receive a call from a fraudster claiming that he is an immigration officer, demanding payment to fix an immigration issue and threatening deportation or imprisonment is payment is not made. The fraudster could also claim that he can help with visa issues or claim to be an immigration lawyer and demands payment.

Internet Purchase Scams

Money is sent by the victim to purchase good purchased online but the goods never arrive. Never send money using a money transfer service for goods or services purchased online.

Flipping Money Scam

The scam starts when people contact, or are contacted by, people pretending to run investment schemes who say they can turn hundreds of pounds into thousands by trading on the stock market or by buying and trading foreign currency. Scammers are asking users for an initial investment of a few hundred pounds and claim that they will receive several times that back in just a few days with the traders taking a small commission. After a few days the victim is informed that there is an issue with returning the profits and more money needs to be sent to return the profits. The victim will never receive and profits and will have lost the investment.

Never entertain individuals that call your out of the blue that are asking you for money. Never send money using a money transfer company.

Military Service Personnel Fraud

This can be linked to a number of different types of fraud where the fraudster pretends to be a military official and tricks individuals to send money.

Social Media Scams

A cyber criminal gains access to your social media account which allows them to use the personal information they can found on the victim in the social media accounts to make requests for money from friends or family members that are connected to the social media account. Social media scams can also involve fake friends that connect socially and make requests for money, free app downloads where personal information is requested, online questionnaires requesting personal information, shortened URL links which do not show the full web address which can install malware on the system.

Always use a strong password on your social media accounts, do not accept friend requests from someone you have not met and do not entertain any requests to download apps, click on links or requests for personal information.

SMS Scam

Texts that request clicking on a link should be avoided as they may take you to a fraudulent site or make requests for personal information.

Tips To Avoid Becoming a Victim of a Scam

Never send money to someone you have not met

Do not send money to someone you have not met for an internet purchase, lottery wins, charity payment, loan offer, job offer, property deposit, police or government official.

If contacted by a relative for an emergency, always call or text the relative

Never give out your transaction reference number or transaction details to anybody outside the intended receiver.

Never send money to someone who is asking you to pay using a money transfer service

Never give out your personal details in response to a request you did not expect

If you have been contacted in relation to a lottery or prize win, ask yourself how you could have won if you did not enter?

Think logically

Resist the pressure to act immediately

Stop and talk to someone you trust

Block unwanted calls and texts

Ask yourself, Is the offer too good to be true? If it is, then it probably is.

Create strong passwords for emails and social media

If you receive an email for personal information, consider them suspicious

Use a strong anti-virus software for your pc and laptop

Avoid using your mobile in public wifi hotspots

Only buy from trusted sources

Only download files and software from trusted sources

Do not use a money transfer service to pay for goods and services.

Remember that cheques take weeks to clear

Do not entertain calls out of the blue for investments or to help you with a debt issue or in relation to any issue you have including virus and malware issues.

Important Note

If you suspect you have become a victim of a scam, contact the police immediately after which, feel free to give us a call. You can also contact action fraud for support, they can be contacted through their website: https://www.actionfraud.police.uk/ and can be contacted via phone on 300 123 2040