FUNDSTR

Fraud prevention

FUNDSTR constantly reviews its fraud and scam prevention systems and is continually developing and deploying new solutions to counter the latest techniques and protect our customers. You, our customers, also have an important part to play in preventing fraud. This information outlines what to do if you suspect you've been targeted by fraudsters, and includes information on the latest scam and fraud techniques, how to protect yourself, and details of how FUNDSTR protects you.

Have you been a victim of fraud?

If you believe you've made a transfer to a fraudster as part of a scam, or you suspect that your account has been subject to fraudulent activity, please:

1. End communication with the suspected scammer immediately (this could be via SMS, WhatsApp, telephone call, email, or in-person contact).
2. Contact the financial institution involved. If that's FUNDSTR, contact us as soon as possible via the Support so that we can help secure your account. Alternatively, you can email us at compliance@fundstr.com. We will prevent any further abuse of your current account. We can cancel or dispute a transfer or a card transaction. We will record the incident and, if necessary, monitor further account activity.
3. Report the incident to the police.

Fraud and scam explained

Fraud: This is usually when criminals use techniques to obtain your account or card details and use those details to make transactions without your knowledge.

FUNDSTR

Scam: These are usually when criminals trick you into making a transaction you suspect to be real, and is instead to them. This typically comes from them pretending to be someone they are not.

Safety recommendations

Here are some of the measures you can take to keep your money safe:

- Be suspicious of ‘too good to be true’ offers or prices.
- Shop with retailers that are reputable and reliable. As a rule of thumb, their website URLs should start with 'https', not 'http'. Look for a padlock icon before the website name, indicating that the site is secured with a digital certificate.
- Never divulge PINs, passwords, one time passcodes or personal details over the phone or to an online chat support.
- Read online reviews to check websites and sellers are genuine, and ask to see high value items in person or via video, as well as getting copies of documentation to ensure the seller owns the item.
- Purchase branded items from the list of authorised sellers listed on their official websites.
- Always access the website you’re buying from by typing it into your web browser. Don’t follow links in unsolicited emails or texts.
- Always ensure you click ‘log out’ or ‘sign out’ of websites
- Remember that fraudsters may ask you to pay by money transfer instead of card payment.
- If you get a message from FUNDSTR saying the payee doesn’t match, stop the transaction and investigate.

Latest fraud and scam techniques

Criminals are using sophisticated techniques to trick people and steal their hard earned money. Here is a list of some, but not all, of the fraud and scam techniques criminals are deploying.

FUNDSTR

Being used as a gatekeeper

The number of young people being used as money gatekeepers is increasing. Criminals use young people who are tempted or forced to move, withdraw or transfer money through their bank accounts. A simple service like transferring money is done in no time and results in fast, easy-to-earn money. But acting as a gatekeeper is a criminal act and can have disastrous consequences.
How to protect yourself from being used as a gatekeeper: Do not allow anyone to use your account to deposit, transfer or withdraw money. Think about whose money it is and what it will be used for. Be suspicious of "job offers" with a promise of fast money and big profits without any need of previous experience. Do not give out your personal ID numbers or banking details.

Remote support or installation of software fraud

This type of fraud occurs when criminals ask you to download software, usually in the form of a mobile or desktop app that typically allows criminals to see your screen or take over your mouse, to gain access to your online or in-app account and transfer money. Fraudsters often use remote access software applications to gain control of your banking and finance applications.

Delivery fee/Customs fraud

The scammers might text you and pretend a parcel is stuck in customs, or pretend a delivery has failed, in order to persuade you to provide important personal information.

CEO fraud

Businesses can also be the victims of fraud. CEO Fraud Criminals impersonate a senior manager in the company and send an email to the accounts department to make a large payment urgently. They often time this so that the manager they are impersonating is away and the details are difficult to verify.

Authorised push payment (APP)

Authorised push payment (APP) is one of the fastest growing types of scams around. This scam involves the fraudster tricking their victims into willingly making large bank transfers to them. For example, they may pose as someone from your bank, or another trusted organisation, claim you have been a victim of fraud and say you need to move your money to a different bank account. Often there is a demand for you to act quickly. Other common scenarios involve a criminal impersonating a conveyancer and stealing money for a house deposit, or pretending to be your builder to steal money saved to pay for renovations.

How to avoid APP scam: If anyone asks you to divert a payment or move your savings – question it to the highest level. Make sure you phone the bank or firm directly and check on any changes to payment details. Don’t rely on emails - they could be intercepted. Never rush a payment, as a genuine organisation won't mind waiting.

Identity theft

Identity theft is when your personal information is stolen and used to open bank accounts apply for plastic cards and loans or for government benefits and documents such as passports, and driving licences in your name.

Criminals can steal your identity in a number of ways, for example finding your credit card or bank statements in your rubbish or stealing your driving licence, cheque book or bank cards. They can use personal details such as your name, date of birth, current and previous addresses and much more to commit identity theft.

Social media can also be used by criminals to access your personal information and build picture of your identity to commit fraud.

Becoming a victim of this type of fraud can mean you will find it difficult to obtain loans, credit cards or mortgages in future.

HOW TO SPOT IDENTITY THEFT:

- Transactions appear on your bank statement that you don't recognize,
- You receive letters about loans, debt or plastic cards you didn't apply for,
- You're told you're already claiming government benefits when you apply,
- You receive bills, invoices or receipts addressed to you for goods or services you haven't asked for,
- A mobile phone contract has been set up in your name without your knowledge.

Investment fraud

You may be targeted by cold callers or presented with fake investment opportunities promoted on search engines and social media sometimes pressuring you to act quickly but also in many cases asking you to leave your details in order for a call back to be arranged. Some may seem genuine because of the use of celebrity endorsements or testimonies from people who've allegedly received large profits but in reality, these are fake.

Criminals often set up cloned websites purporting to be legitimate investment firms and may even send out paperwork with official branding to add a layer of credibility to their scams. You may also receive an initial payment or even a couple of payments with "returns" on your investment to convince you to invest larger sums of money. These scams include convincing you to invest in markets such as gold, property, carbon, cryptocurrencies such as Bitcoin or even wine.

HOW TO SPOT INVESTMENT FRAUD:

- You see ads within your social media feeds, sometimes celebrity endorsed, offering high returns on investments,

- You’re contacted out of the blue by phone, email or social media about an investment opportunity,
- You may be offered a high return on your investment with apparently little or no risk,
- You’re told the investment opportunity is exclusive to you,
- If an offer sounds too good to be true, then it probably is,
- For some types of investment, you’re pressurised into making a decision with no time for consideration.

Do not get in touch with a scammer – they are very good manipulators who can easily influence people. Be cautious of approaches presenting you with exclusive investment opportunities. The investment process should be in written form and documented, not a verbal ‘agreement’ over the phone. It’s important that you do your research and proceed with extreme caution before making any investments. Check the respective Authority’s register for regulated firms, individuals and bodies.

Serious companies that comply with the law are not allowed to advertise financial investments with overpraise and should always disclose the risks of investments. Scammers rarely do, which is another reason to hang up the phone or report the internet ad. Moreover, people who have been deceived by these fraudsters sometimes get calls from someone who claims to cooperate with Interpol and offers to track down the fraudsters, but is actually the same fraudster who wants to attract additional sums.

Fraudsters are capitalising on the growing excitement around cryptocurrency, by asking you to move money and offering fake investments. How to stay safe:

- stay in control - never let anyone set up a cryptocurrency wallet, upload ID documents or manage investments for you.
- don't share access - fraudsters may ask you to download software so they can access your devices and move money without your knowledge.
- spot familiar tricks - you may be asked to move money, but to give your bank another reason to get a 'smoother' transaction. Fraudsters know payments for investments may attract more scrutiny and will try to avoid it.
- don't fall for fake endorsements - fraudsters may impersonate famous people on social media or messaging groups, to make their offer look legitimate.

- don't be pressured - high value cases even give a return in the short term, to convince you to invest more. Then, after larger payments are sent, the victim suffers even greater losses.
- Never mislead your financial institution about the purpose of a payment. Criminals will often try to persuade you to write in the transactional subject line that the payment is for something different to what they have told you. They may suggest it will go through smoother or the financial institution may stop the payment otherwise. This is a clear sign of fraud.

Romance fraud

You're convinced to make a payment to a person you've met either through social media platforms, dating websites and apps or gaming sites. Fake profiles are used by criminals in an attempt to build a relationship with you. Criminals use information found on social media to create fake identities to target you with a scam, looking for profiles that say you're 'widowed' or 'divorced'. They often go to great lengths to gain your trust and convince you that you're in a genuine relationship before appealing to your compassionate side to ask for money. Criminals will 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 you if they are overseas.

HOW TO SPOT ROMANCE FRAUD:

- You've met someone online and they declare strong feelings for you after a few conversations,
- There are spelling and grammar mistakes, inconsistencies in their stories and they make claims such as their camera isn't working,
- They suggest moving the conversation away from the dating website or social media to a more private channel such as email, phone or instant messaging,
- Their profile on the internet dating website or their social media page isn't consistent with what they tell you,
- They refuse to video call/meet you in person,
- Photos generally tend to be stolen from other people,

- You're asked to send money to someone you have not met face-to-face, either through bank/money transfer or through the purchase of gift cards or presents such as phones and laptops. You may even be asked to provide them with access to your bank account or card.
- Upon questioning your friend or family member, they may become very secretive about their relationship or provide excuses for why their online partner has not video called or met them in person. They might become hostile or angry, and withdraw from conversation when you ask any questions about their partner.
- They try to persuade you to make an investment, often saying it is easy or guarantees high returns.

ALWAYS REMEMBER:

- Avoid sending money to someone you've never met in person, particularly if you have only recently met online.
- Research the person you're talking to as profile photos may not be genuine. You can do this by uploading a picture of the person you're talking to into your search engine to check that profile photos are not associated with another name. Performing a reverse image search can find photos that have been taken from somewhere, or someone, else.
- Be alert to spelling and grammar mistakes and inconsistencies in stories.
- Stay on the dating sites messaging service until you're confident the person is who they say they are and meetings in person take place in a public place.

Fake invoice fraud

This is a method where fraudsters send invoices of varying amounts by email. A company or individual receives an invoice for a service or goods that they have not ordered/purchased. The fraudster hopes that the person/company will not check the invoice and make the transfer.
Fraudsters use bank accounts in various banks.
How to protect yourself:

- Be careful and check the content of the invoices sent to you.

- If the sender of the email is unknown, do not open the email (it may contain malware).
- If the name of an actual company is used in the invoices, inform the company that false invoices are being sent in its name.
- Do not reply to the sender and inform the police. If you have made a transfer to the fraudster, also report the incident to your financial institution.

IBAN fraud

The fraudsters usually target companies (mainly those that cooperate with foreign companies and make regular transfers), but also private individuals. The mailbox of the partner company is hacked and then used to learn information or monitor invoicing. The victim company is then notified of a change in the bank account details of the partner company at the appropriate time and an 'invoice' with the current account number of the fraudster is submitted. Sometimes, the partner company immediately submits an invoice for the service/products without information about the change of details. Fraudsters usually use private companies to commit fraud. However, they may also pretend to be a public authority, i.e. it seems like a public authority is submitting an invoice.

How to protect yourself:

- Verify the international bank account number (IBAN).
- If you learn about a change in the details by phone or email, be suspicious of the caller/sender. If necessary, ask specifying questions and compare the structure and content of the emails with previous ones.
- Be suspicious of changes in details and contact your business partner to confirm the updated details before making a payment.
- If you discover a fraud, report it to your management, business partner, your financial institution, and the police.

Lottery fraud

Lottery frauds are committed on the Internet and social media. Often, fraudsters use the name of a well-known company or a name similar to it. For example, they may pretend to be a telecommunications company that is giving away an expensive mobile phone. They send an email or a message on social media to the victim, claiming they have won a prize even though they have not even participated in the game/campaign. When the victim clicks on the ad, they are asked to submit their personal data, to make a payment, to enter their bank account or bank card number, etc.
How to protect yourself:

- Be very cautious about messages claiming you have won something. Do not click on them.
- Do not disclose personal information (bank account, bank card numbers, social security number, date of birth, address, etc.) or make money transfers. If you are asked for them, it is a fraudulent message.
- Fraudsters often use these kinds of messages to gain access to the device (computer, phone) of the victim. If you click on the ad, the fraudster may be able to install malware on your device.
- Report the incident to the police and, if you have made transfers to the fraudster, also your financial institution.

Phishing

How To Recognize Phishing: Scammers use email or text messages to try to steal your passwords, account numbers, or Social Security numbers. If they get that information, they could get access to your email, bank, or other accounts. Or they could sell your information to other scammers. Scammers often update their tactics to keep up with the latest news or trends, but here are some common tactics used in phishing emails or text messages: Phishing emails and text messages often tell a story to trick you into clicking on a link or opening an attachment. You might get an unexpected email or text message that looks like it's from a company you know or trust, like a bank or a credit card or utility company. Or maybe it's from an online payment website or app. The message could be from a scammer, who might say they've noticed some suspicious activity or log-in attempts — they haven't, claim there's a problem with your account or your payment information — there isn't, say you need to confirm some

personal or financial information — you don't, include an invoice you don't recognize — it's fake, want you to click on a link to make a payment — but the link has malware, say you're eligible to register for a government refund — it's a scam, offer a coupon for free stuff — it's not real.

Here are signs that this email is a scam, even though it looks like it comes from a company you know — and even uses the company's logo in the header:

- The email has a generic greeting.
- The email says your account is on hold because of a billing problem.
- The email invites you to click on a link to update your payment details.

While real companies might communicate with you by email, legitimate companies won't email or text with a link to update your payment information. Phishing emails can often have real consequences for people who give scammers their information, including identity theft. And they might harm the reputation of the companies they're spoofing.

How To Protect Yourself From Phishing Attacks:

Your email spam filters might keep many phishing emails out of your inbox. But scammers are always trying to outsmart spam filters, so extra layers of protection can help. Here are four ways to protect yourself from phishing attacks:

1. Protect your computer by using security software. Set the software to update automatically so it will deal with any new security threats.

2. Protect your cell phone by setting software to update automatically. These updates could give you critical protection against security threats.

3. Protect your accounts by using multi-factor authentication. Some accounts offer extra security by requiring two or more credentials to log in to your account. This is called multi-factor authentication. The extra credentials you need to log in to your account fall into three categories:

something you know — like a passcode, a PIN, or the answer to a security question.

something you have — like a one-time verification passcode you get by text, email, or from an authenticator app; or a security key

something you are — like a scan of your fingerprint, your retina, or your face.

Multi-factor authentication makes it harder for scammers to log in to your accounts if they do get your username and password.

4. Protect your data by backing it up. Back up the data on your computer to an external hard drive or in the cloud. Back up the data on your phone, too.

Payment in advance fraud

Also known as an advance fee scam, this is when you're convinced to pay an upfront fee in order to receive a prize/service, high-value goods or loans which never materialise.

HOW TO SPOT A PAYMENT IN ADVANCE SCAM:

- You're asked to pay an upfront fee to receive money, a prize/service or goods that you weren't expecting,
- You're asked to pay an upfront fee for a training programme or background check for a job that may not exist,
- You're told that fees are fully refundable and will be used as a deposit, administrative charge or for insurance,
- There are follow-up fees you need to pay in order to secure the loan, prize/service or goods,
- You are put under pressure to pay quickly by wire, bank transfer or cryptocurrency,
- The domain name doesn't match that of the sender of the email.

ALWAYS REMEMBER:

- Question claims that you're due money for goods or services that you haven't ordered or are unaware of, especially if you have to pay any fees upfront,
- It's extremely unlikely that you've won a lottery or competition that you haven't entered, and which requires an upfront fee,
- Check the email addresses of recruiters or potential employers to ensure they're genuine and be vigilant of those platforms that businesses would be unlikely to use i.e. Yahoo, Hotmail or Gmail,
- Confirm the organisations you're being contacted by are registered on enterprise register and use the details provided to contact companies and/or organisations directly,
- Be wary of potentially fake profiles on social media platforms such as LinkedIn as they could be offering jobs that don't exist.

FUNDSTR

Purchase fraud

Online shopping provides criminals with an opportunity to trick people into paying for goods and services that don't exist, often advertised via auction sites or social media with images taken from genuine seller's to convince you they're the real deal. Criminals also use cloned websites with slight changes to the URL to trick you into thinking you're purchasing from the genuine site. They may also ask for payment prior to delivery and send you fake receipts and invoices that appear to be from the payment provider.

Types of fraud include buyers paying deposits for pets that don't exist, DIY equipment purchases and electronic devices such as games consoles, mobile phones and other devices. Another tactic criminals use to trick people into falling for fraud is to ask for payment for courier services or insurance when buying and selling online.

HOW TO SPOT PURCHASE FRAUD:

- You're offered a heavily discounted or considerably cheaper product or service compared to the original items genuine worth. The deals often sound too good to be true.
- You're asked to pay by bank transfer instead of using the online platform's secure payment options.
- You receive a fake email receipt/invoice that appears to be from the website you've purchased from or the payment service used to make your purchase. The email address domain doesn't match that of the genuine sender's.
- The website that you're purchasing from was only launched days/weeks ago.
- A sense of urgency is placed on ordering the product or service so that you don't miss the price/deal.

ALWAYS REMEMBER

- Be suspicious of any "too good to be true" offers or prices.
- Use the secure payment method recommended by reputable online retailers and auction sites.
- Read online reviews to check websites and sellers are genuine, and ask to see high value items in person or via video link, as well as getting copies of the relevant documentation to ensure the seller owns the item.