Frauds & Scams - An Overview

Fraudsters and scammers are always finding new ways to make money, and here at Omni we'll share these on our website so our customers can learn from them and be extra vigilant.

If you ever believe you are a victim of fraud or have fallen victim to a scam, you should contact the relevant companies as soon as possible which typically may include:

- **Omni Capital Retail Finance** – Our contact page should be completed so our fraud specialists can investigate this further and get to the bottom of the situation.
- **Bank/Credit Card Company** – It is important to contact your bank/credit card provider so they can put a block on future transactions and investigate the allegations.
- **Action Fraud** – Action Fraud is the UK's national reporting centre for fraud and cybercrime where you should report fraud if you have been scammed, defrauded, or experienced cybercrime in England, Wales and Northern Ireland. Action Fraud's website can be found at https://www.actionfraud.police.uk/what-is-action-fraud.

What is the difference between Frauds & Scams?

Put simply, a fraud is something that happens **to you** verses scams which happen **with your help** (either knowingly or unknowingly).

Lets explore these a little further.

Fraud

Fraud tends to happen when a fraudster gets hold of your personal details often (but not always) by illegal ways, such as:

Term	Explanation/Example
Phishing	The fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.
Vishing	The fraudulent practice of making phone calls or leaving voice messages purporting to be from reputable companies in order to induce individuals to reveal personal information, such as bank details and credit card numbers.
Data breach	A data breach is a security violation, in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorised to do so. Other terms are unintentional information disclosure, data leak, information leakage, and data spill.

Scams

One of the toughest things about being scammed, is at the time, you probably wouldn't realise it is even happening.

The risk of being scammed lies within anything we do including, but not limited to, Crypto Currency Investments, NFT's (Non-Fungible Tokens) purchases, Romance Scams, Get Rich Quick Schemes or Business Investments. Whenever we share information with someone, we run the risk of it being a scam.

To bring this example to life, we have spoken to several customers who thought they were opening crypto currency trading accounts. Unfortunately, instead they simply provided all of their personal information (including a copy of their passport or driving license) to a fraudster, who then applied for loans and credit in their name.

Before you consider sharing your information with anyone, take five minutes, really look at the situation, and check you understand the risks. It is so important to ensure you are dealing with a genuine company and that there is a logical reason for why they are requesting the information that they want.

In these situations, sometimes it helps to think about what advice would you give a friend of yours? For example:

- What if they told you they could make a lot of money by simply sharing their password and ID with an individual online?

- What questions or concerns would you share with them?

Remember that this is your personal information, your details, your ID document, therefore your money at risk.

Have you ever heard the phrase 'Money Mule'?

A 'Money Mule' is an individual who transfers stolen money between different bank accounts. A Money Mule, on occasions, is not aware that their actions are a criminal offence.

That said, even if you're unaware that the money you received was illegally obtained, the fact that you participated in the movement of the money means that you can still be prosecuted.

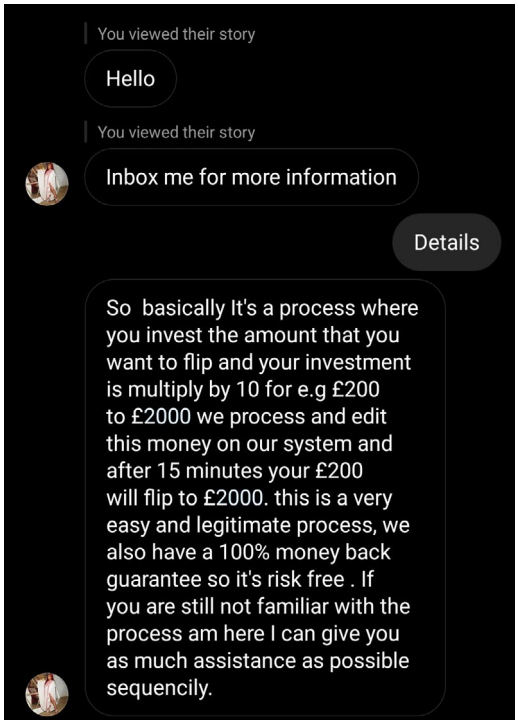
Example of a Money Mule offer

Peter received a new follower on Instagram.

He didn't think too much of this as it was not out of the ordinary to receive notifications like this.

Peter clicked on the individual's profile and saw the following images.

Soon after he viewed the profile, Peter received a direct message from the account. He asked for more details to learn about the investment:



Peter has seen several of these images before and understands that this is likely to be a scam. If he wasn't aware of these scam approaches, then within a few minutes he could have shared his information and suffer a substantial financial loss.

The old phrase of "if it's too good to be true, it probably is" is even more appropriate in this day and age!

Types of frauds/scams

We are supportive of the 'Take Five' national campaign which is offering straight-forward, impartial advice that helps prevent email, phone-based and online fraud. Their website is very detailed and worth a read to get some understanding of fraud types. There are some examples below (with links to the Take Five website) which might give you an idea of how fraudsters can obtain your personal information.

- **Identity Theft** - ID theft is when your personal information is stolen and used to open bank accounts, take out credit cards and loans or apply for government benefits and documents in your name such as passports and driving licences.

- **Investment scam** - You're convinced to move your money into a fictitious fund or account, or to pay for what later turns out to be a fake investment.

- **Impersonation scam** - You're convinced to make a payment or give personal and financial details to someone claiming to be from an organisation you trust. This could include the police, your bank, a delivery or utility company, communication service provider or a government department such as HMRC or the DVLA.

- **Purchase Scam** - The increase in online shopping has provided criminals with an new 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 sellers' to convince you they're the real deal.

- **Romance Scam** - 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 – this is also often known as catfishing.

- **Banking Fraud** - Can occur through three channels: online, telephone and mobile banking. To commit this fraud criminals gain access to your bank account and make unauthorised transfers of money.

- **Doorstep Scam** - A cold-caller may offer you a service you don't really need. They may claim to have noticed something about your property that needs work or improvement, such as the roof, and offer to fix it for cash or an inflated price.

- **Holiday Scams** - From fake caravans or motorhome listings to "too good to be true" offers for holidays, villa rentals and holiday lets, criminals use a variety of methods to trick us into handing over our money and information.

Handy hints to spot a scam?

- **Ask yourself "am I expecting this email, and has it been sent from a genuine domain name?"**
  - Do you have an existing relationship with this firm or person and if not, is there any information about them online without having to click a link they've provided themselves? Often, anything that is fraudulent will not have a credible online presence.
  - Genuine firms will rarely use a free webmail account such as hotmail.com or gmail.com. Also watch out for company email accounts that have had a character added, or swapped round.
  - Omni will only ever email you from an email address ending in @ocrf.co.uk.

- **If it's too good to be true, it probably is!**
  - Some of the emails or texts you receive about amazing offers may contain links to fake websites that steal personal information. If you're unsure, don't use the link and either:
    - type a website address that you trust directly into the address bar
    - use a trusted search engine and follow the search results
  - 'Get rich quick schemes' are almost always scams and victims stand to lose a lot of money - crypto currency is particularly popular at the moment.
  - Don't be fooled by time-limited offers that encourage you to act very quickly – this is often a technique to get you to click on a link more quickly, and pay less attention to the risks.

- **Is the website secure?**
  - When the time to pay for your items online, check there's a 'closed padlock' icon in the browser's address bar.
  - If the padlock icon is not there, or the browser says not secure, then don't use the site. Don't enter any personal or payment details or create an account.

- **Should this person be asking for this information?**
  - Unless you are dealing with someone you already know and trust, no one should ask to access your computer/mobile phone remotely, or for your pin or passwords.
  - Stop and think before you send any payment, money or vouchers to people you don't know or have only recently met. Scammers can be quite persuasive and will gain your trust to get your money!

One last reminder...

Remember, if you would like to report a fraud allegation to Omni please complete our contact page and we will be in touch to discuss further.

Castle Trust Bank

Omni Capital
Retail Finance