Hillingdon Fraud & Cyber Crime Summary

December 2020

Executive Summary

Number of offences	191
Total loss	£409,073
Average per victim	£2,142

Top 5

The top 5 by **volume** (number of reports) type of fraud is as follows:

Fraud Type	Amount of Offences	Amount Lost
Online Shopping and Auctions	45	£25,376
Misc. (False Representation)	28	£94
Other Advance Fee Frauds	23	£4,224
Other Consumer Non Investment Fraud	16	£35,066
Cheque, Plastic Card and Online Bank Accounts (not PSP)	11	£25,562

The top 5 by **amount** reported lost:

Fraud Type	Amount Lost	Amount of Offences
Mandate Fraud	£101,639	5
Share sales or Boiler Room Fraud	£53,644	4
Fraud by Abuse of Position of Trust	£50,253	3
Pyramid or Ponzi Schemes	£40,000	1
Other Consumer Non Investment Fraud	£35,066	16

Fraud Advice

Payment Fraud (aka Mandate Fraud)

Payment fraud is a specific type of fraud which targets businesses with the intention of getting them to transfer money to a bank account operated by the criminal.

There are two main types of payment fraud, **CEO fraud** and **Mandate Fraud**. Both are usually targeted at staff within a company's accounts department and use spoofed sender email addresses (sometimes called Business Email Compromise)

CEO fraud involves an email that claims to be from a senior member of staff within a company such as a CEO (Chief Executive Officer). The email will ask the receiver to make a payment or transfer funds for an ongoing or new business transaction. Often the payment request is marked as urgent and pressure is applied to the receiver to make the payment as soon as possible.

Mandate fraud involves an email which appears to come from a known supplier. The email will request that future payments for products or services are made to a new bank account and give a reason for the account change.

In each instance, the new account will be under the control of the criminal and any funds paid in to it will be lost.

How to protect yourself

If an email is received requesting a change of bank details on an account or a one off payment, verify this by making direct contact with the organisation or person requesting the change. Ideally, phone them on a number you already have, failing that, double check the email used. Do not use any contact details from the suspicious email. Don't be pressurised by any email, or follow up phone call, as this may be the criminal. Always double check.

However, some criminals are getting wise to this, and so will prep a victim in advance by contacting them a few days or weeks earlier to change any stored phone numbers or emails to their own. So, it's a good idea to double check any contact when change of details occur. Make sure you double check via the original contact details.

REMEMBER – Don't change bank details without double checking.

CAUTION – Sometimes, criminals will call in advance to fraudulently change contact numbers. Check when these change too.

THINK - Why does this payment have to be made?

Other Consumer Non Investment Fraud

Sometimes businesses use deceptive business practices that can cause their victims to suffer financial losses.

The victims believe they are participating in a legal and valid business transaction when they are actually being defrauded. Fraud against consumers is often related to false promises or inaccurate claims made to consumers, as well as practices that directly cheat consumers out of their money.

How to protect yourself
• Research the company before purchasing goods or services.
• Use Companies House to find out how long they have been trading.
• Ensure you use trusted, reviewed companies.
• Avoid using direct bank transfers when purchasing items online, instead use a credit card.

Fraud by Abuse of Position of Trust

When someone abuses their position of authority or trust for personal or financial gain, or so that someone else loses money or status.

Friends, family members, carers or company employees may be asked to look after your personal or business finances. They may instead take advantage of their access to bank accounts or information for their own benefit, or misuse the assets of a business to embezzle funds for themselves.

How to Protect Yourself

- Make sure you have complete confidence in anyone you entrust with your finances to make decisions on your behalf. Don't be afraid to change your mind in future.

- Grant the trust to more than one person to make joint decisions (so everyone in the position of trust has to agree on decisions together).

- You'll need to be prepared to challenge suspicious behaviour if you've been given a position of trust alongside someone else.

- If you're being pressured into making a decision by someone you've given a position of trust to or being intimidated or told to keep certain dealings secret from other trustees, then make sure you speak to someone else you trust.

Pyramid or Ponzi Schemes

Pyramid scheme fraud involves an unsustainable business which rewards people for enrolling others into a business that offers a non-existent or worthless product.

A fraudster advertises a multi-level investment scheme that offers extraordinary profits for little or no risk. You're required to pay a fee to enter the investment scheme.

You're then required to recruit friends or family members to enter the scheme. If you do this successfully, you're paid out of their receipts. They are then told to recruit others to keep the chain going.

Your money is not actually invested in any product. Instead, it's simply passed up the chain of investors. Because pyramid schemes are unauthorised and make no profits, you're very unlikely to recover any lost investment. While the fraudster at the top will collect most of the profits, those who entered the scheme later end up losing out. Legitimate trading schemes rely on valuable goods and services, while illegal pyramid schemes focus simply on recruiting more and more investors.

Using hard-sell techniques, fraudsters try to pressure you into making rushed decisions, giving you no time to consider the nature of the investment.

Fraudsters aim to make their business seem legitimate. This means they will often use technical jargon, impressive job titles and mock websites to look credible. If you have any suspicions about a scheme's authenticity, you should investigate the company's status and contact details.

How to Protect Yourself

- If you're considering any type of investment, always remember: if it seems too good to be true, it probably is. High returns can only be achieved with high risk.

- Pyramid schemes often involve products that are overpriced and have no real resale value. You should think about the true

Investment Fraud

Investing in stocks and shares or any other commodity can be a successful way of making money. However, it can also lead to people losing their entire life savings. Fraudsters will persuade you to invest in all kinds of products. They will offer you high rates of return, particularly over longer periods of time, which often do not exist.

Common products that will be offered include binary options, virtual currency, carbon credits, wine, rare metals, gemstones, land and alternative energy. Often, initial investments will yield small returns as an incentive to invest further funds. However, larger investments or cashing out will be met with excuses or a penalty charge. Eventually contact with the fraudster will be impossible and all funds and bogus returns lost.

Fraudsters are organised and they may have details of previous investments you have made or shares you have purchased. Knowing this information does not mean they are genuine.
Criminals may direct you to well-presented websites or send you glossy marketing material. These resources do not prove they are a genuine company. Many fraudulent companies have a polished customer image to cover their illegal activities.

It is relatively easy to register a company with Companies House. This does not confirm or endorse that they can provide genuine investments. Indeed, emerging investment markets may be unregulated, making these open to abuse.
Companies may be registered at prestigious addresses, for example Canary Wharf or Mayfair. This does not mean they operate from there. It is an accepted business practice to rent such a virtual office to enhance a business's status. However, fraudsters are also aware of this and exploit it.
The fraudster may put pressure on you by offering a 'once in a lifetime opportunity' or claim the deal has to be done quickly to maximise profit.

In addition - be wary of companies that offer to 'recover' any funds you have lost to any sort of investment scam.

They may be linked to the company who initially defrauded you in the first place and may be targeting you again. This is known as 'Recovery Fraud'.

How to protect yourself

- There are no get rich quick schemes. If it sounds too good to be true, it probably is.
- Genuine investment companies will not cold call you. Be extremely wary of anyone who does.
- Research both what you have been offered, and the investment company. Speak to Trading Standards if you have concerns.
- Before investing, check the Financial Conduct Authority register (https://register.fca.org.uk/) to see if the firm or individual you are dealing with is authorised
- Check the FCA Warning List of firms to avoid.

REMEMBER - Don't be pressured into making a quick decision.

CAUTION - Seek independent financial advice before committing to any investment.

THINK - Why would a legitimate investment company call me out of the blue?

Remember:

Your bank, the police, or tax office will **never** ask you to attend your bank, withdraw, transfer or pay money over the phone or send couriers to collect your card or cash. Nor would they ask you to buy goods or vouchers.

This is a scam.

1. **Hang up** (Never give details or money following a cold call)
2. **Take 5** (Seek a second opinion, tell someone what has happened)
3. **Verify** (if concerned, contact the company via a pre-confirmed method)

All of our videos and electronic leaflets can be found on the following link; www.met.police.uk/littlemedia
Free cyber advice can be found https://www.ncsc.gov.uk/cyberaware/home

Always report, Scams fraud and cyber crime to Action Fraud,
either online at **www.actionfraud.police.uk** **or by telephone on 0300 123 2040.**

STOP
Taking a moment to stop and think before parting with your money or information could keep you safe.

CHALLENGE
Could it be fake? It's ok to reject, refuse or ignore any requests. Only criminals will try to rush or panic you.

PROTECT
Contact your bank immediately if you think you've fallen for a scam and report it to Action Fraud.