Westminster Fraud & Cyber Crime Summary

November 2019

Executive Summary

Number of offences		176
Total loss	£	2,998,505
Average per victim	£	17,037

Top 5

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

Fraud Type	Amount of Offences	Amount Lost
Misc. (False Representation)	26	£0
Online Shopping and Auctions	23	£84,587
Cheque, Plastic Card and Online Bank Accounts (not PSP)	21	£1,032,453
Mandate Fraud	16	£412,511
Other Consumer Non Investment Fraud	13	£10,173

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

Fraud Type	Amount Lost	Amount of Offences
Cheque, Plastic Card and Online Bank Accounts (not PSP)	£1,032,453	21
Mandate Fraud	£412,511	16
Corporate Procurement Fraud	£400,000	2
Fraud by Abuse of Position of Trust	£265,429	6
Rental Fraud	£263,483	12

Fraud Advice

Online Shopping and Auction Sites

Online shopping can save you time, effort and money. Millions of people use websites such as eBay and AutoTrader to buy new or second hand goods for competitive prices. These sites give you the opportunity to purchase a huge choice of goods from all over the world. However, among the genuine buyers and sellers on these sites, there are criminals who use the anonymity of the internet to offer goods for sale they do not have, or are fake.

In the majority of transactions, the buyer and seller never meet. Which means when making a purchase or sale on a website, you are reliant on the security measures of the site.

Fraudsters will advertise an item for sale, frequently at a bargain price compared to other listings of a similar type. They may have pictures of the item so it appears to be a genuine sale.

A favoured tactic is to encourage buyers to move away from the website to complete the transaction, and the criminal may offer a further discount if you do so. Many websites offer users the opportunity to pay via a recognised, secure third party payment service, such as PayPal, Android Pay or Apple Pay. Read the website's advice and stick to it. Fraudsters might be insistent you pay via bank transfer instead. By communicating and paying away from the website, contrary to their policies, you risk losing any protection you had.

Criminals may also email or contact you if you have 'bid' on an item but not been successful in winning the auction. They will claim that the winning bidder pulled out or didn't have the funds and offer you the chance to buy the item. Once you agree, they will either provide bank details or even insist payment is made via a third party payment service for mutual protection. Once you agree, they 'arrange' this. You then receive a very legitimate looking email which appears to be from the website or a third party payment service directing you how to make the payment. Some are very sophisticated, even having 'Live Chat' functions that you can use to speak to a sales advisor! Unfortunately, you will again be communicating to the fraudster, so beware!

In both these scenarios, once the payment is made, the 'seller' won't send the item. They'll either not reply to you or make excuses as to why they haven't sent the goods.

If they do send the item, they'll send counterfeit goods instead of the genuine items advertised. Again, you may struggle to receive any compensation or resolution to this problem from the legitimate website, as it could be against their policies.

Fraudsters also use e-commerce websites to pose as 'buyers.' If you have an item for sale, they may contact you and arrange to purchase this. It is common for criminals to fake a confirmation that payment has been made. Before posting any item, log in to your account via your normal method (not a link on the email received) and check that you have received the money.

You must also be careful what address you send items to. Fraudsters may ask you to send items to a different address. They may claim they need it sent to their work address or to a friend or family member. If you send the item to an address other than the one registered on the user account, you may not be provided any protection from the website or payment service.

How to protect yourself

- Stay on site!
- Be wary of offers that look too good to be true.
- Read the consumer advice on any website you are using to make a purchase. Use the recommended payment method, or you may not be refunded for any losses to fraud.
- Research the seller/buyer and any of their bidding history.
- Don't be convinced by pictures, they may have been taken from somewhere else on the internet. You can check photos using a reverse image search on the internet through websites like www.tineye.com or https://reverse.photos
- Be suspicious of any requests to pay by bank transfer or virtual currency instead of the websites recommended payment methods.
- Never buy a vehicle without seeing it in person. Ask to see the relevant documentation for the vehicle to ensure the seller has ownership.
- If you are selling online, be wary of any emails stating funds have been sent. Always log in to your account via your normal route (not via link in email) to check.
- Watch our video on Online Shopping Fraud at www.met.police.uk/littlemedia .

  REMEMBER - Stay on site.
  CAUTION - Be wary of paying by bank transfer or virtual currency.
  THINK - Why is this item so cheap? Is it a scam?

Banking and Card Fraud - Online Banking

The use of online banking or people using banking apps on smartphones and tablets has grown. People use them at home or when they are out and about.

To stay safe while banking online you must protect your password and personal details to stop criminals from accessing your accounts. Many banks provide one-time passcodes sent to your device when setting up new

payments. These should never be shared with anyone, even from the bank. If you're speaking to your bank on the phone, and they ask you for it, you are certainly speaking to a criminal, not your bank.

How to protect yourself

- Choose, use and protect passwords and memorable words with great care. Watch our video on passwords at www.met.police.uk/littlemedia for further advice.
- Keep online banking software and banking apps up to date. Always download updates when prompted.
- When logging in whilst in public, take extra care to shield any PIN codes or passwords.
- Always log out of your online banking account or banking app when you have finished using it. Closing the app or web page or turning off your device may not be sufficient.
- Do not use publicly available Wi-Fi networks for banking. It is very difficult to tell if a hotspot is secure.
- Don't share any security codes with anyone.
- If your bank has called you. Take a reference number, and then hang up before recalling on a number you know to be safe after a few minutes to clear the line.

Payment 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?

Rental Fraud

Sometimes, criminals advertise properties to rent when these properties don't belong to them, or even don't exist! Victims are then tricked into paying an upfront fee to rent the 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.

How to Protect Yourself

- Do not send money to anyone advertising rental properties online until you are certain the advertiser is genuine.
- If you need to secure accommodation in the UK from overseas, seek the help of the employer or university you are coming to, or get a friend, contact or relative to check the property exists and is available.
- Do not pay any money until you or a reliable contact has visited the property with an agent or the landlord.
- Ask for copies of tenancy agreements and any safety certificates such as Gas Electricity or HMO Licence.
- Do not be pressurised into transferring large sums of money. Transfer funds to a bank account having obtained the details by contacting the landlord or agent directly after the above steps have been followed.
- Be sceptical if you're asked to transfer any money via a money transfer service like Western Union.

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.getsafeonline.org

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