Explanation of types of fraud/scam offences currently being seen

What is Courier Fraud?

Courier fraud occurs when a fraudster contacts victims by telephone purporting to be a police officer or bank official. To substantiate this claim, the caller might be able to confirm some easily obtainable basic details about the victim such as their full name and address.

The caller may also offer a telephone number for the victim to telephone or ask the victim to call the number on the back of their bank card to check that they are genuine. In these circumstances, either the number offered will not be genuine or, where a genuine number is suggested, the fraudster will stay on the line and pass the victim to a different individual.

After some trust has been established, the fraudster will then, for example, suggest;

- Some money has been removed from a victim's bank account and staff at their local bank branch are responsible.

- Suspects have already been arrested but the "police" need money for evidence.

- A business such as a jewellers or currency exchange is operating fraudulently and they require assistance to help secure evidence.

Victims are then asked to co-operate in an investigation by attending their bank and withdrawing money, withdrawing foreign currency from an exchange or purchasing an expensive item to hand over to a courier for examination who will also be a fraudster.

At the time of handover, unsuspecting victims are promised the money they've handed over or spent will be reimbursed but in reality there is no further contact and the money is never seen again.

What is Investment Fraud?

When you get a cold call from someone pretending to offer you the opportunity to invest in a variety of schemes or products that are either worthless or don't even exist.

It's also known as share sale fraud, hedge fund fraud, land banking fraud or bond fraud.

The majority of investment frauds are run out of offices known as boiler rooms.

What is a Rogue trader/Doorstep Criminal?

Doorstep crime includes trader's cold calling at your door and claiming that work needs doing to the home or garden. They may prey on insecurities by saying there is a safety risk if the victim leaves the work undone. If the victim agrees to let them go ahead, the work is usually neither carried out or it is completed badly and the price is put up because they pretend to have found extra things that needed doing.

Common types of cold calls include:

Your roof or guttering is damaged – when in reality it may not be

Trees on your property are unsafe and need attention – they may or may not be unsafe, but consult a qualified tree surgeon to find out

Your roof has moss on it which needs cleaning – the National Federation of Roofing Contractors advises that moss on a roof is not a problem and that this service is completely unnecessary

Your driveway needs cleaning – if you agree then the trader may persuade you to have other areas cleaned too, pushing up the price from the original estimate.

Recovery Scams.

The Fraudster contacts the victim, usually by phone or email, and tells them they are a solicitor, a law enforcement officer or someone working for a government agency in another country.

They tell the victim that they know they have already lost money to a fraud and they can recover their money for them. Alternatively, they might claim that the fraudsters who initially conned them have been convicted, the money they took has been seized and it is due to be returned to their victims.

If the victim responds to their offer of help, they will ask for various fees. For example: release fees, administration fees etc. If they pay these fees, they will keep coming back with another fee that has to be paid before they can return the money.

If victim asks them to take the fees from their money they claim to have recovered, they will give reasons why this isn't possible. For example: your money is under the control of a court and can only be paid back to you personally.

The fraudsters will also ask the victim to provide details of their bank account so that they can pay the money into it but instead will use this information to defraud the victim's bank account.

Romance Scams.

When the victim thinks they have met the perfect partner through an online dating website or app, Facebook etc., but the other person is using a fake profile to form a relationship with them. The fraudster uses the site to gain the victims trust and eventually asks them for money or enough personal information to steal the victim's identity.

Once the fraudster using a fake dating profile is confident that they've won the victims trust, they will tell them about a problem they're experiencing and ask them to help out by sending money.

They may have arranged to visit to the victim, but need money to pay for the flight or visa. They may tell them everything has been booked but their ticket has been stolen, and they need to send money quickly to get them on the next flight.

Alternatively they may prey on their sympathies, telling them a family member or someone else they are responsible for is ill and they need money for medical treatment.

Once the victim sends them money, the fraudsters will keep coming back and invent new reasons to send them more.

Latest HMRC scams.

- Fraudsters are contacting the elderly and vulnerable claiming to be from HM Revenue & Customs.
- Victims are being told they have arrest warrants, outstanding debts or unpaid taxes in their name.
- The fraudsters are asking victims to purchase iTunes gift cards as payment.
- There are a variety of methods being used including calls, texts and voicemails.

Victims are being contacted in a variety of methods by fraudsters claiming to be from HMRC and are being told they owe an outstanding debt. In most cases they ask for payment in iTunes gift card voucher codes.

Fraudsters like iTunes gift cards to collect money from victims because they can be easily redeemed and easily sold on. The scammers don't need the physical card to redeem the value and instead get victims to read out the serial code on the back over the phone.

One 87 year old victim recently told the BBC he was phoned by fraudsters who claimed to be from HMRC stating there was an arrest warrant out in his name. They told him it would be cancelled if he bought £500 in iTunes gift cards at Tesco. The man bought the cards and gave them the serial numbers but when they asked for a further £1,300 in vouchers, he became suspicious and hung up.

Latest TV licence Scams.

The scam email claims to offer a refund for over-payments of TV Licence fees, but states the victim's bank details need to be updated before the refund can be issued.

The email then links to a website designed to look like TV Licensing's own website with a form for victims to enter their details. In reality the website has been set up to look authentic but the form steal victim's bank details, giving the fraudsters the chance to steal the victim's savings.

These types of scam are likely to become more prevalent with mobile phones over the coming months as we approach over 75's having to pay for their TV licences in the future.

Amazon Prime Scams

Unsuspecting members of the public are targeted with automated calls which tell them a fraudster has used their personal details to sign up for an Amazon Prime subscription. The victim is then instructed to press 1 to cancel the transaction. When they do this, they are directly connected to the real scammer who poses as an Amazon customer service representative.

The criminal tells the victim the Amazon Prime subscription was purchased fraudulently and that they need remote access to the victim's computer in order to fix a security flaw that will prevent it from happening again. The victim is instructed to download an application called Team Viewer and asked to log onto their online banking account. The software download grants the fraudster remote access to the victim's computer and allows them to see the victim's personal and financial details.

Other variants of the crime involve victims being told they are due a refund for an unauthorised

transaction on their Amazon account or telling victims their subscription will be 'renewed' for £39.99. The call will then say that you should 'press 1' to speak with an 'account manager'.

Do not press 1, simply hang up immediately. Amazon will never contact you in this way, and the call being completely unsolicited should also set off alarm bells.

Unsolicited requests to remote access your computer should always raise a red flag, as once in to your PC they can gain access to all your personal data. If you've received an unexpected phone call, or other communication, stop and take a minute to think about whether an organisation would get in touch with you out of the blue in this way. Instead, contact them directly using a known trusted email address or trusted phone number. Never use a telephone number supplied by the caller or an email address. Never divulge personal details/data over the phone.

Prevent & Protect Fraud Office
Essex & Kent Serious Crime Directorate
Rayleigh Police Station

Email: chloe.rudd@essex.police.uk
Ext: 490312
Mob: 07966 476233

ESSEX POLICE
Protecting and serving Essex

TAKE FIVE TO STOP FRAUD

SECURE
PROTECT
PREVENT