Recent Scam/Fraud Items

The following is a list of scams which you should be aware of :-

Pension Scam Alert – Cape Verde

The National Fraud Intelligence Bureau (NFIB) has been alerted to a pension scam whereby cold callers continue to target members of the public aged 50 to 60 years old to release and transfer their pension early. Suspected firms who advertise and arrange pensions are offering investments in alternative commodities such as hotel developments or property in Cape Verde, and operate as unregulated collective investment schemes.

Often, the cold calling 'pension companies' involved are neither regulated nor qualified to give financial advice and classify themselves as a 'trustee', 'consultant' or an 'independent advisor' and offer exceptionally high return rates for investors.

Some victims have signed documents that authorises a limited company to be set up using their personal details, including utilising a Small Self–Administered Scheme (SSAS). Whilst SSAS accounts and limited companies are essential for legitimate schemes, the fact that victims are unaware that this will happen suggests that the scheme may not have been fully explained to them, increasing the likelihood that there may be an element of fraud involved.

Protect yourself:

Further advice can be found at:
http://www.fca.org.uk/your-fca/documents/protect-your-pension-pot
http://www.fca.org.uk/consumers/financial-services-products/pensions/protect
http://www.thepensionsregulator.gov.uk/individuals/dangers-of-pension-scams.aspx

Ensure that you request that the risks and growth rates are explained and that you fully understand them before transferring your pension

Check whether the pension arrangement company is registered with the FCA. Registered companies can be checked using the FCA register online at:
https://register.fca.org.uk/

Remember that if the offer seems too good to be true, then it generally is

If you believe that you have been a victim of fraud you can report it online http://www.actionfraud.police.uk/report_fraud or by telephone 0300 123 2040.

Action Fraud – Telephone Number Spoofing

Fraudsters are using a scam to make the people they are phoning believe they are speaking to a trusted organisation by fooling their phones into displaying any number they choose.
Full details can be found on the following link - http://www.actionfraud.police.uk/news/alert-watch-out-for-new-number-spoofing-scam-oct14

Intercepting Replacement Bank Cards

The National Fraud Intelligence Bureau's (NFIB) Proactive Intelligence Team is warning people of a new method of fraud whereby fraudsters are exploiting the delay in the replacement of victims' bank cards by intercepting their mail. According to the NFIB, fraudsters have identified that if a genuine banking customer requests a new card to replace a damaged one, some banks will send the replacement card but not cancel the damaged card straight away, leaving it active for several days. Fraudsters target letterboxes in communal flats and premises that lack security and CCTV to steal victims' mail, specifically banking documentation. Having identified a victim via the stolen letters and open source information, fraudsters have all the personal information they need. The fraudster calls the bank pretending to be the customer. They state that the plastic bank card has snapped but is still functioning, and that they will need a replacement sent to their home address. The fraudster returns a few days later to steal the bank card contained within the mail and utilises it for fraudulent purposes. Victims won't become aware of the fraud until several days later when their original card stops working and they get in touch with their bank.
Research conducted for Action Fraud's "Not With My Name" campaign found that 71% of people do not regularly redirect their post for at least six months when they move house. Also, 1 in 3 people don't shred letters before throwing them away. This leaves people vulnerable to bank statements and other mail being intercepted by fraudsters. A convicted fraudster told the NFIB, "identity fraud is dead easy, it's like any scam, you just need to plan it through. Do your homework, think it out, keep it simple and look for the system flaws".
Protection advice from the 'Not With My Name' campaign:

- Always destroy or securely store personal documents.
- Check your bank and financial statements carefully and report anything suspicious to the bank or financial service provider concerned. When getting rid of personal documents always destroy them – rip up or shred.
- If you have a communal mailbox or one in a shared area, empty it frequently.
- If you move home set up a redirection with Royal Mail for at least a year and notify your bank, credit card companies and other organisations you deal with ASAP.
- Personally assess your communal mail area for vulnerabilities and consult with your premises management team about implementing added security measures.

Council Tax Scam

This is a message sent via The Neighbourhood & Home Watch Network (England & Wales).
This information has been sent on behalf of Action Fraud (National Fraud Intelligence Bureau)

(Please do not reply directly to this email, please use the Reply button at the bottom of this message)

Message sent by

Action Fraud (Action Fraud, Administrator, National)

Fraudsters have been phoning victims telling them that they have been placed in the wrong council tax bracket for a number of years and are entitled to a rebate. They normally say that this rebate should be worth about £7,000. Once the victim is convinced, the fraudster tells them that in order to receive the rebate they will need to pay an administration fee in advance. The payment they ask for varies between £60–£350. The victim provides the details and makes the payment, but then is no longer able to make contact with the person they spoke to on the phone. When they phone their council about the rebate and the fact that they are in the wrong tax bracket, the council will confirm that they know nothing about it and that they have been contacted by fraudsters.

The fraudsters have mainly been targeting both male and female victims who are aged 60 and over and live in the Sussex area, but it is likely that the fraudsters will also start to target victims in other areas.

Protect Yourself:

- Never respond to unsolicited phone calls.
- Your local council won't ever phone out-of-the-blue to discuss a council tax rebate. If you receive a call of this nature, put the phone down straight away.
- No legitimate organisation will ask you to pay an advanced fee in order to receive money, so never give them your card details.
- If you think you have been a victim of fraud, hang up the phone and wait five minutes to clear the line as fraudsters sometimes keep the line open. Then call your bank or card issuer to report the fraud. Where it is possible use a different phone line to make the phone call.

Buy Back Diamond Scam

The National Fraud Intelligence Bureau's (NFIB) Proactive Intelligence Team is warning people of a new scam dubbed "diamond buy-back courier fraud". Information gathered by the intelligence team suggests that boiler rooms operating from overseas (specifically in Thailand) are targeting existing investors of diamonds from 'victim sucker lists' circulated by fraudsters internationally.
Existing clients who have purchased genuine but lesser value diamonds are contacted by fraudsters who ask if they would like to increase the value of their investment, as the return on their current stock has been so good. They are encouraged to purchase more diamonds and invest further – buying either overpriced or non-existent diamonds.
In this new type of scam, the victim is contacted and informed that the value of diamond(s) they have physically purchased have significantly increased due to the rarity and demand. They are then convinced that in order to revalue the diamond(s) they will need to be physically returned to be assessed by a fake "valuation team". Victims are then offered a free of charge, no hassle return service to undertake the valuation process. Intelligence suggests the fraudsters use UPS (United

Postal Service) to collect the diamond(s). The fraudsters have no intention of returning the diamonds.

Protect yourself against investment fraud

- If you're considering any type of investment, always remember: If it seems too good to be true, then it probably is. High returns can only be achieved with high risk.
- If you get a call out of the blue, be wary. If in doubt, don't be polite, just hang up.
- Take the time to seek independent legal or financial advice before making a decision.
- Always verify the credentials of the company you're dealing with. Check for known fraudulent organisations with the FCA.