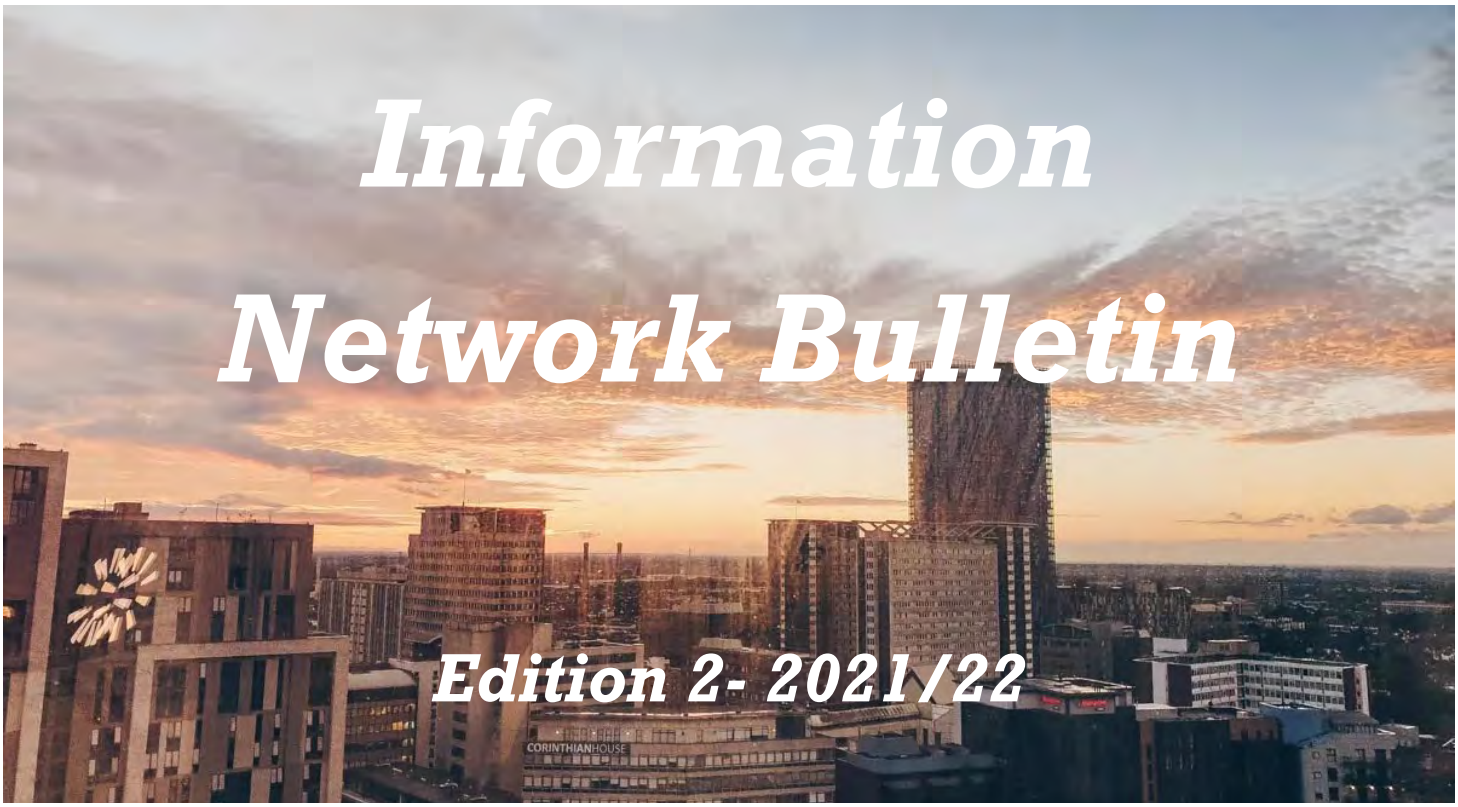

Welcome to the latest edition of the Information Network Bulletin brought to you by Croydon Council's Trading Standards team.
In addition to general news from the team, it includes details of some of the latest scams and fraud alerts which we have become aware of in recent months.

We hope that you find it useful.

Criminals are using the NHS COVID Pass as a way to target the public by convincing them to hand over money, financial details and personal information.

They are sending imitation text messages, emails and making phone calls pretending to be from the NHS, and offering fake vaccine certificates for sale online and through social media.

If you are contacted about your NHS COVID Pass:

1. Be alert to links and attachments in unexpected text messages or emails
2. Do not respond to requests for money, passwords or financial details
3. Challenge: Could it be fake?
4. Use the official NHS COVID Pass website (see below)

The NHS COVID Pass is available to demonstrate your COVID-19 status either in a digital or paper format via the NHS App, the NHS website or by calling 119.

For information on how to get your **free** NHS COVID Pass, visit www.nhs.uk/nhscovidpass.

What to do if you suspect you have been a victim of an NHS COVID Pass scam

If you receive a call and suspect it to be fraudulent, hang up. If you are suspicious about an email, forward it to report@phishing.gov.uk. If you are suspicious about a text message, forward it to the number 7726, which is free-of-charge.

If you believe you are the victim of a fraud, please report this to Action Fraud as soon as possible by visiting actionfraud.police.uk or calling 0300 123 2040.

If you have any information relating to NHS COVID Pass or vaccine certificate fraud you can stay 100% anonymous by contacting Crimestoppers online at covidfraudhotline.org or phone on 0800 587 5030.

COVID Vaccine & Digital Vaccine Passports

There has also been an increase in fraudulent sites designed to imitate official NHS websites where the links and look of the website are very similar to the genuine sites – these are often designed not only to defraud people financially but also to harvest personal information that can later be used in further fraud such as applying for loans or credit cards or setting up bank accounts.

The NHS has been targeted by fraudsters purporting to be able to produce 'digital vaccine passports'. People have been reporting scam emails and text messages purporting to be from the NHS which contain a link that takes you to a copycat website where you have to fill in a form giving your personal information. Action Fraud want to remind people of the following:

- **The NHS will never ask you for your bank account or card details.**
- **The NHS will never ask you for your PIN or banking passwords.**
- **The NHS will never arrive unannounced at your home to administer the vaccine.**
- **The NHS will never ask you to prove your identity by sending copies of personal documents such as your passport, driving licence, bills or pay slips.**

www.actionfraud.police.uk/vaccine

The overriding message is to be very careful of which websites you visit. Do not rely on links which are sent in emails and texts where you cannot be sure who sent the message. Go the official website directly yourself and search up the service needed.

If you have fallen victim to a fraud please report it to Action Fraud on 0300 123 2040 or report on line at https://www.actionfraud.police.uk/reporting-fraud-and-cyber-crime. If you have given financial information or made a payment please contact the relevant financial institution (bank or credit card provider) to make them aware and to report the issue.

Use PayPal? Watch out for ‘over-sending’ scams!

Reports are being made nationally about fraudsters manipulating the PayPal system to defraud people of their goods and money.

The fraud commences when the fraudulent ‘purchaser’, makes their purchase and claims that they have sent to ‘seller’ too much.

For example, someone may be selling phone for £300, but the fraudster will send £500 and pretend it is a mistake. They will then ask the seller to send the additional money, the extra £200, back to them.

Once the seller has sent back the £200.00, the fraudster will lodge a complaint with PayPal claiming that their account has been compromised and that they never meant to send the money in the first place.

PayPal will then urge the seller to send back any money received, leaving the seller out of pocket. Even if they haven’t sent to item to the purchaser yet, they will have lost the ‘overpaid amount’ that they sent back.

Or you may receive a spoofed email saying that you’ve been paid £500 for the phone that you listed as £300; followed by an email from the ‘purchaser’ asking that you ship the phone together with the extra £200 that you were paid by mistake.

Don’t fall for it!

Log into your PayPal account and check that you really have been paid before sending anything.

When you log into your account to check that payment has been received, don’t use the link from the email advising of the payment. We recently received a report from a Croydon resident who received an email advising that payment had been received for a phone she was selling. She accessed her account via the link in the email and saw the payment was there, so she posted the phone to the purchaser. She then received an email advising that she had to pay £150 to upgrade her PayPal account to receive the money she had been paid. Suspecting this to be a scam, she accessed her PayPal account via another route and saw that no money had been received for the phone that she had posted and was now unable to retrieve. So whilst she didn’t fall for the second scam, she still lost her phone and the money she would have received for it.

Do exercise caution when buying and selling online.

Protect yourself from scammers, thieves, and hackers by watching out for warning signs.

You can also sign up for PayPal's Seller Protection Program, and PayPal will monitor transactions for signs of fraud.

A potentially life threatening TikTok trend, involving tiny magnets that can be easily swallowed, has triggered the NHS to call for a ban.

These tiny magnetic balls are widely sold as creative toys, with a recent TikTok craze seeing them used as fake facial piercings by teenagers. The viral prank sees people place two magnetic balls either side of their tongue and wiggle it around, creating the illusion that their piercing is real.

The NHS issued a patient safety alert after at least 65 children were admitted to hospital for urgent surgery in the last three years after swallowing magnets. The magnetic objects are forced together in the intestines or bowels, squeezing the tissue so that the blood supply is cut off. Ingesting more than one can be life-threatening and cause significant damage within hours. These magnets which are less than 6mm in diameter are powerful in magnetism and can be easily swallowed.

The Office for Product Safety and Standards (OPSS) has also warned of the risk of serious injury and death from swallowing small high-powered magnets. OPSS has identified a particular hazard arising from the use of high-powered magnets in products, where the magnets can be swallowed, such as fridge magnets, earrings, tongue piercings and drink charms. Businesses and online platforms have been reminded of their obligations under product safety law.

They must remove from the market products containing small magnets which breach the safety requirements of the Toy Safety Regulations or the General Product Safety Regulations. Specifically, businesses and retail platforms are advised to remove from the market any products that breach the magnetic flux index where there is a risk that magnets may be ingested by a child.

They must also ensure that clear warnings are included with any products that contain magnets, where there is a risk of ingestion.

The public is being asked to take appropriate steps to keep these products away from children as ingestion could result in a serious or fatal injury. Parents or guardians should understand the signs of magnetic ingestion and act quickly to get immediate medical treatment if they believe a magnet has been swallowed.

Scams Training

Friends Against Scams is a National Trading Standards Scams Team initiative, which aims to protect and prevent people from becoming victims of scams by empowering people to take a stand against scams.

Learn how to protect yourself and your loved ones from scams. Complete the Friends Against Scams awareness session and help to raise awareness throughout your community.

Please use the link below to the online Scams Awareness session and help Croydon Trading Standards raise awareness and protect our residents:

www.friendsagainstscams.org.uk/elearning/Croydon

WATCH OUT!

PENSION SCAMS ABOUT

Pension scams can be hard to spot. Scammers can be articulate and financially knowledgeable, with credible-looking websites, testimonials and materials that are hard to distinguish from the real thing.

How pension scams work

Scammers usually contact people out of the blue via phone, email or text, or even advertise online. Or they may be introduced to you by a friend or family member who is also unknowingly being scammed.

Scammers will make false claims to gain your trust. For example:

- claiming they are authorised by the FCA or that they don't have to be FCA authorised because they aren't providing the advice themselves

claiming to be acting on the behalf of the FCA or the government service Pension Wise (link is external)

Scammers design attractive offers to persuade you to transfer your pension pot to them (or to release funds from it). It is then often invested in unusual and high-risk investments like overseas property, renewable energy bonds, forestry, storage units, or simply stolen outright.

Scam offers often include:

- free pension reviews
- higher returns – guarantees they can get you better returns on your pension savings
- help to release cash from your pension even though you're under 55 (an offer to release funds before age 55 is highly likely to be a scam)
- high-pressure sales tactics – the scammers may try to pressure you with 'time-limited offers' or even send a courier to your door to wait while you sign documents
- unusual investments – which tend to be unregulated and high risk, and may be difficult to sell if you need access to your money
- complicated structures where it isn't clear where your money will end up
- arrangements where there are several parties involved (some of which may be based overseas) all taking a fee, which means that the total amount deducted from your pension is significant
- long-term pension investments – which mean it could be several years before you realise something is wrong

4 simple steps to protect yourself from pension scams

Step 1 - reject unexpected offers

If you're contacted out of the blue about a pension opportunity, chances are it's high risk or a scam.

If you get a cold call about your pension, the safest thing to do is to hang up - it's illegal and probably a scam. Report pension cold calls to the Information Commissioner's Office (ICO) (link is external).

Be wary if you're contacted about any financial product or opportunity and they mention using your pension.

If you get unsolicited offers via email or text you should simply ignore them. Fortunately, most people do reject unsolicited offers – FCA research suggests that 95% of unexpected pension offers are rejected.

Be wary of offers of free pension reviews. Professional advice on pensions is not free – a free offer out of the blue (from a company you have not dealt with before) is probably a scam.

And don't be talked into something by someone you know. They could be getting scammed, so check everything yourself.

Step 2 - check who you're dealing with

Check the FCA Register to make sure that anyone offering you advice or other financial services is FCA authorised.

If you don't use an FCA-authorised firm, you also won't have access to the Financial Ombudsman Service (link is external) or Financial Services Compensation Scheme (FSCS) (link is external) so you're unlikely to get your money back if things go wrong. If the firm is on our Register, call our Consumer Helpline on 0800 111 6768 to check the firm is permitted to give pension advice.

Check they are not a clone – a common scam is to pretend to be a genuine FCA-authorised firm (called a 'clone firm'). Always use the contact details on our Register, not the details the firm gives you.

Check to see if they are registered with Companies House (link is external) and for the names of the directors. Search the company name and the names of the directors online to see if others have posted any concerns.

Check the FCA Warning List – use this tool to check the risks of a potential pension or investment opportunity. You can also search to see if the firm is known to be operating without our authorisation.

Step 3 - don't be rushed or pressured

Take your time to make all the checks you need – even if this means turning down an 'amazing deal'. Be wary of promised returns that sound too good to be true and don't be rushed or pressured into making a decision.

Step 4 - get impartial information or advice

You should seriously consider seeking financial guidance or advice before changing your pension arrangements.

- The Pensions Advisory Service provides free independent and impartial information and guidance.
- If you're over 50 and have a defined contribution pension, Pension Wise offers pre-booked appointments to talk through your retirement options.
- You can also use a financial adviser to help you make the best decision for your own personal circumstances. If you do opt for an adviser, make sure they are regulated by the FCA and never take investment advice from the company that contacted you, as this may be part of the scam. Find out more about getting financial advice

If you suspect a scam, report it

If you have been a victim of this type of fraud, report it to Action Fraud by calling us on 0300 123 2040 or by using our online reporting tool.

- Report to the FCA – you can report an unauthorised firm or scam to the FCA by contacting their Consumer Helpline on 0800 111 6768 or using our reporting form.
- You can report nuisance calls and messages to the Information Commissioner's Office using their online reporting tool or by calling 0303 123 1113.
- If you've agreed to transfer your pension and now suspect a scam, contact your pension provider straight away. They may be able to stop a transfer that hasn't taken place yet. If you are unsure of what to do contact the Pensions Advisory Service) for help.
- If you have already invested in a scam, fraudsters are likely to target you again or sell your details to other criminals. The follow-up scam may be completely separate or related to the previous fraud, such as an offer to get your money back or to buy back the investment after you pay a fee.

Cryptocurrency fraud leads to millions in losses so far this year

Data from Action Fraud, the national reporting centre for fraud and cyber crime, reveals a staggering £146,222,332 has been lost to cryptocurrency fraud since the start of this year – which is almost a third more (30 per cent) than was lost throughout the whole of 2020.

What is cryptocurrency fraud?

Cryptocurrency is a digital or virtual currency designed to work as a medium of exchange. Cryptocurrencies are known for their market volatility so the value of investor's assets go up and down quickly. As more people have invested their money in cryptocurrencies, criminals have capitalised on this as an opportunity to commit fraud.

Criminals advertise schemes promising, in some cases, high returns through cryptocurrency investing or mining. Frequently advertised on social media, criminals try to lure you in with adverts offering easy money quickly in order to obtain your money or personal information.

How to protect yourself

- Be wary of adverts online and on social media promising high returns on investments in cryptoassets or cryptoasset-related products and be suspicious if you are contacted out the blue about an investment opportunity. This could be via a cold-call, an e-mail or an approach on social media.
- Don't be rushed into making an investment. No legitimate person or firm will pressure you into making an investment, or committing to something on the spot. Take time to do your research.
- Most firms advertising and selling investments in cryptoassets are not authorised by the Financial Conduct Authorotiy (FCA). This means that if you invest in certain cryptoassets you will not have access to the Financial Ombudsman Service or the Financial Services Compensation Scheme if things go wrong – so always check the FCA Register to make sure you're dealing with an authorised firm and check the FCA Warning List of firms to avoid.
- Seek advice from trusted friends, family members or independent professional advice services before making a significant financial decision. Even genuine investment opportunities can be high risk.
- Use a financial advisor accredited by the Financial Conduct Authority. Paying for professional advice may seem like an unnecessary expense, but it will help prevent you from being scammed.
- Only use the telephone number and email address on the FCA Register, not the contact details the firm gives you and look out for subtle differences.
- Just because a company has a glossy website and glowing reviews from 'high net worth' investors does not mean it is genuine – fraudsters will go to great lengths to convince you they are not a scam.
- Remember, if something sounds too good to be true, it probably is.

If you think you've been a victim of an investment fraud, report it to Action Fraud online at www.actionfraud.police.uk or by calling 0300 123 2040. For more information about investment fraud, visit www.fca.org.uk/scamsmart.

Driving Licences

There has been a rise in the proliferation of third party 'check & send' services for UK driving licences. These are services which you can carry out directly via the gov.uk web services or via the Post Office Check & Send services.

Many of the third party service providers charge over and above what you would pay if you did it directly with the DVLA or Post Office. These third party companies are not affiliated with the DVLA and cannot get your documents or requests processed any quicker. There are also companies that whilst they appear to be UK based are actually based abroad and therefore not subject to the same legislation and data protection laws. Given that you are providing sensitive data in order to complete the transaction and receive your documents, you need to be sure you can trust who you are giving this information to. Consider if your information could be used fraudulently as you are providing your personal details.

Many of the websites do include a disclaimer somewhere on the site stating they are not affiliated with the DVLA but it is not obvious, especially when some of the sites are almost 'copycat' versions of official sites.

Last year the DVLA urged motorists to beware of websites that charge a premium for DVLA online services that are cheaper or free on GOV.UK. The agency reminded motorists that they should always use GOV.UK, to be sure they are dealing directly with DVLA and not paying more than they need to.
For further information see the full article: https://www.gov.uk/government/news/motorists-warned-of-websites-charging-a-premium-for-dvla-services-free-on-govuk

GOV.UK state 'applying online will always be the quickest, easiest and often cheapest way to transact with DVLA – and by going to GOV.UK motorists can be sure their application is safe and secure'. Visit the following link for information on how to renew your licence, change an address, and replace a lost or stolen licence - https://www.gov.uk/browse/driving/driving-licences

Illicit Tobacco & Singles Cigarettes Sales

Croydon Trading Standards are continuing their work on eliminating illegal tobacco from the borough. If you are aware of any shops selling illegal tobacco that includes counterfeit and non-duty paid cigarettes or hand-rolling tobacco, foreign brands of cigarettes with no legal market in the UK and banned oral tobacco, [please report them to us. In addition, sales of single cigarettes are also illegal and we would like to know if this is taking place. Please follow the instructions below to report any illegal selling to us.

The main way to report any issue to Trading Standards in the first instance is via the Citizens Advice Consumer Advice line on 0808 223 1133 or via their 'Chat Service' or via an online reporting form – all found at https://www.citizensadvice.org.uk/consumer/get-more-help/if-you-need-more-help-about-a-consumer-issue/

If you want to anonymously report consumer crime, or a business that you are aware is trading illegally or unfairly to Trading Standards, you can do this via a number of means.

Via the London Trading Standards online reporting form found at:
http://www.londontradingstandards.org.uk/contact/

You could also report via Crime Stoppers on 0800 555 111 or via their online reporting tool at:
https://crimestoppers-uk.org/ - this may take longer to reach us.

You can also contact Croydon Trading Standards directly at Trading.Standards@croydon.gov.uk but please be aware this will not be anonymous and you will receive an automated message giving you the details of the Consumer Advice Line.

Pet Fraud

During the COVID-19 pandemic there has been a marked increase in online scams.

These include 'Pet scams' where people advertise puppies and kittens online on sites such as Pets4Homes, Gumtree and groups on FaceBook but these animals do not exist – they are simply a fraud.

Other frauds revolve around people buying dogs (and some cats) where they are given false information in regards to their place of birth, their age and vaccination status and even their breed. There has been a big influx in puppies being smuggled from Ireland into Northern Ireland and into the UK. These puppies are often unvaccinated, ill, too young to travel or be taken away from their mothers and have been poorly treated; sadly many do not survive. Many are also the result of backyard breeding schemes where the health of the dogs involved is low priority and the breeders are out to make as much money as possible with breeders often concealing their real identity making it very difficult to get any redress or refunds when the puppies fall ill or die leaving new owners facing extortionate vet bills and the dogs involved suffering.

Action Fraud state that **£2,638,323** was lost by prospective pet owners in the 2020/21 financial year, after they put down deposits for pets they saw advertised online – an increase of over 20 per cent compared to the previous financial year.

Please do your research properly if you are looking to get a pet and consider using a reputable breeder or rescue centre where you can see reviews about the service other customers have received, ask lots of questions about the animals and if buying from a breeder see the animal in person before you part with any money. Recent legislation states that any puppies or kittens should be viewed with their mother.

Lucy's Law means that anyone wanting to get a new puppy or kitten in England must now buy direct from a breeder, or consider adopting from a rescue centre instead. It also means that licensed dog breeders are required to show puppies interacting with their mothers in their place of birth. Please be aware that some unscrupulous scammers bring in female dogs to act as the puppies' mother – then give excuses as to why the dog is not acting in a normal motherly manner. Scammers are also known for using COVID as an excuse to why you cannot visit the puppies and try to arrange collection in a place away from the address eg a car park. https://www.gov.uk/government/news/lucys-law-spells-the-beginning-of-the-end-for-puppy-farming
If anyone you are considering buying from is evasive, gives excuses as to why you cannot visit a premises or suggests you part with money before seeing the puppy – act with caution and do not part with any money. Please also consider carefully how you pay – cash or bank transfer means you have no buyer protection and will be unable to get your money back in the event of a fraud or dispute whereas using PayPal or a Credit Card does give you some protection.

https://getyourpetsafely.campaign.gov.uk/ is the Government campaign to give advice to people considering buying a pet and to help avoid potential pet owners from being 'Petfished'.

Fraudsters continue to target persons using cash machines to withdraw money

Fraudsters are tampering with cash machines in an effort to con people out of their money.

Scammers are currently using dual purpose cash machines to access withdrawals, duping customers into believing there is only one box for both withdrawals and deposits by concealing the ATM's withdrawal slot with a plastic cover.

Having put in their card, pin number and the amount of cash that they want to withdraw, the customer is then led to believe the cash point is out of service because no money is dispensed. They are unaware that there's actually a separate slot for the cash they are withdrawing to emerge from.

When the customer walks away, the scammer can then approach the machine, open the cover over the correct dispenser and take the money.

In one instance, scammers had even put a sign up above the ATM that said deposits were currently out of service. This led the customer to assume the deposit box was the same box that his cash should have been dispensed out of - which was currently out of order.

Banks and building societies advise customers to always check for suspicious activity before withdrawing cash in public.

It is important that people remain vigilant and check for any suspicious devices when using ATMs, especially those located outside. Using a cashpoint is easy, convenient and almost always safe. But sometimes criminals tamper with cash machines to steal your card information, PIN, or cash.

Always be vigilant when using an ATM - look out for any signs it might have been tampered with or damaged but also be aware of covering your PIN and 'shoulder surfers' hanging around

Was this bulletin helpful?

Contact Trading Standards to request a free door sticker advising cold callers that they are not welcome. If you are a victim of scam mail, contact us to receive a free copy of our toolkit on how to avoid falling victim and how to stop the letters.

Additionally, please let us know what you think of this bulletin and what Trading Standards topics you would like to see covered in future editions.

Contact Trading Standards: Tel: **020 8407 1311**
Email: **trading.standards@croydon.gov.uk**

Citizens Advice Consumer Service: Tel**: 0808 223 1133**
Web: **www.citizensadvice.org.uk**