Information Network Bulletin

March 2025 Edition

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.

New Authorised Push Payment Fraud Reimbursement Protection

Authorised Push Payment fraud is a devastating crime that happens when you are persuaded to pay money from your account to a fraudster's account with a bank transfer. The transfer could have happened online, by phone or a transaction that you arranged in the bank branch. And the money could have been sent to someone that you are in a romance with, where you're asked to pay someone you have never met, or where the fraudster pretended to be a police officer or bank official and persuaded you to transfer your money to their so called 'safe' account.

New protections have been in place since 7th October 2024, and these cover individuals, small businesses and charities. The maximum amount that can be claimed back is £85,000, but if your claim is for more than that amount and your bank does not reimburse the additional money, you could raise a case with the Financial Ombudsman Service. Their financial limit is much higher, £420,000 but remember the Ombudsman Service views each case on an individual basis.

To claim a reimbursement under the new rules, contact your bank immediately. They will be able to help you and guide you through the process. You should report the details of your fraud to the police and/or give your permission for the bank to report it to the police on your behalf. You should also report the matter to Action Fraud, and you can get further support following this crime, from Victim Support or from Citizens Advice.

You can find out more by asking your bank or building society or from UK Finance: https:\\www.ukfinance.org.uk/authorised-push-payment-fraud-reimbursement
(Also see page 9 of this bulletin for a guide to reimbursement)

Rogue Traders are Cold Calling in your Area

Rogue Traders are active in the Croydon area. They carry out leaflets drops, cold call by door knocking, or advertise on online platforms.

Checks on many traders reported to Citizens Advice show they often fraudulently use logos or claim membership to industry associations such as Checkatrade. Sometimes they are members, but as these are paid membership schemes where minimal meaningful checks are undertaken it is hard to know if they are legitimate traders. Other platforms are simply paid adverts or paid access to potential customers such as Bark.com where no checks are carried out prior to them being allowed to use the platform.

They also use fake addresses. The addresses often exist but are mail forwarding services or offices which the 'traders' are not based at and have no permission to use. They also create companies on Companies House and create fancy looking websites; but this does not mean they are genuine traders.

They quote a small amount then start raising the costs to do unnecessary work. They are often unskilled and their 'work' will result in damage to your property or you having to pay for remedial work. They are also likely to fly tip any waste locally.

Please DO NOT engage with, or use the services of, anyone who cold calls.

We have also had reports of aggressive, rude and forceful behaviour. If traders are aggressive, threatening or intimidating, always call the police on 999.

If you receive a flyer and want to report it to Trading Standards, please take a photo and email it to us at trading.standards@croydon.gov.uk

If you require a trader, please look at the following **Approved Trader Schemes**:

Trust Mark - www.trustmark.org.uk/find-a-tradesman - **0333 555 1234**

Buy With Confidence – www.buywithconfidence.gov.uk – **01392 383 430**

Which? Trusted Traders - http://trustedtraders.which.co.uk/ - **0117 405 4689**

ALWAYS get several quotes in writing from several traders before having any work done. Ensure it includes a breakdown of costs of labour and materials and comprehensive cancellation rights, terms and conditions. If you have an emergency – please do not automatically use Google and contact the first results – these are often paid for adverts and increasingly they appear to be linked to rogue traders.

If you have been scammed or duped into contracting with a business or a trader and parted with money, please report to **Citizens Advice Consumer Advice Line on 0808 223 1133** or go to the following website to report online:

https://www.citizensadvice.org.uk/consumer/get-more-help/if-you-need-more-help-about-a-consumer-issue/

Croydon Trading Standards Team wins Team of the Year!

Croydon Council's trading standards team have been recognised by the London Trading Standards by being awarded Team of the Year.

The awards, held annually, celebrate the achievements of dedicated officers across 10 award categories.

Croydon trading standards were recognised for their vital work as part of Executive Mayor Jason Perry's priority to make the borough a cleaner, safer and healthier place to live and work in.

The awards described Croydon's trading standards team as succeeding in doing 'what they do best – protecting consumers, enforcing the law and supporting decent businesses'.

London Trading Standards praised the council's team for its efforts over the past year. It recognised that the service had seized thousands of illicit vapes, undertaken hundreds of age-restricted product test purchases, investigated many doorstep crime cases, and intervened in a number of scam victims' cases.

London Trading Standards also praised Croydon's team for successfully developing relationships with schools, and advising and educating parents, teachers and pupils on the dangers of vapes.

Stuart Radnedge, London Trading Standards' Regional Coordinator, said: "The awards are the chance to recognise the work of such amazingly talented individuals and teams who do their upmost to protect everyone in London."

"Warmest congratulations to our trading standards team – we're all proud of their hard work and this award is very well deserved."
Jason Perry, Executive Mayor of Croydon

Illicit Tobacco in Croydon

Croydon Trading Standards are continuing our work to remove illegal tobacco from the borough.

If you are aware of any shops or traders selling illegal tobacco, which 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, or any traders selling singles, please report them to us.

The sale of illegal tobacco products undermines legitimate traders, puts peoples health at risk and puts traders at risk of prosecution and having their alcohol licence reviewed if they are found to be supplying illegal products.

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 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/

Alternatively, you can email us at trading.standards@croydon.gov.uk

Shop fined over £20,000 for illegally selling vapes

Croydon Council is cracking down on illegal traders in the borough following another prosecution and fine of over £20,00

The shop owner in Thornton Health sold a vape to an underage person and ignored basic health regulations.

Link Telecom was fined £2,500 for selling a vape to a person under-age at a shop on Brigstock Road, as well as £20,000 for two offences for failing to display health warnings. The ruling also ordered they pay the council's legal costs of £5,008.13.

No one from the company showed up at the court hearing, so they were convicted in absence. The ownership of the business has recently changed hands which the court called a 'cynical' attempt to abuse the court process. The business owner has six months to pay the fine.

Jason Perry, Executive Mayor of Croydon, said: "I'm proud that we have the best Trading Standards team in London because they work hard to protect residents and businesses against illegal operators. "Our Trading Standards team do really important work to help keep us all safe. Residents are vital in helping the team, so if anyone thinks a shop is selling restricted products to those underage or illegal vapes, please get in touch."

Business can contact the council if they would like more information to deter underage sales or any other trading standards assistance.

Digital Wallet Fraud

Banks are reporting a rise in Apple Pay and Google Pay being set up fraudulently, which means that criminals can access victims card details through their digital wallets. As such, they are giving out advice to help their customers protect themselves from these frauds.

What the fraud looks like:

- Bob sees a social media sale advert, apparently by a well-known company.
- Tempted by the offers, he makes a purchase and enters the usual card payment information to make the transaction.
- The website then asks him to authenticate the payment using a one time passcode.

  So he follows the instructions given on the page and completes the order.

What has really happened:

Bob has entered his card and personal information into a fake site. This information was then used by a criminal to add Bob's card to their digital wallet. The one time passcode Bob received wasn't for the card payment, it was to register the digital wallet. This gave the criminal access to Bob's card to make purchases through their digital wallet.

Here are some steps you can take to avoid this happening to you:

- **Always read the full one time passcode message**

  The message will explain what the code is for. If the message doesn't match with what you're trying to do, **STOP** and call your bank.
- **Turn off AutoFill on your device**

  Change your device settings to stop codes, such as one time passcodes, being entered automatically without opening and reading the full message.

Cont.

Digital Wallet fraud (Cont.)

- **Check it out**

  Do your own research of the company and check their website directly. If they have a sale on, it will be included on their website too. Don't just trust that a social media ad is genuine.

Remember:

- Once a criminal has your details, they can use them to commit further, more costly scams.
- They can use the information to pretend to be your bank or the police.
- **If anyone contacts you and asks you to move your money to keep it safe, it's a SCAM.**

Report of Grooming by Local Conman

A local resident recently contacted Croydon Trading Standards after losing a few thousand pounds to a trader who was going to construct a shed for her to store her e-bike in. In speaking to the consumer, it became apparent that she had been groomed by the gentleman who had pleaded hardship in order to encourage her to give him work and help support his family. The resident had met the 'handyman' via some friends she had made on a social media site. These 'friends' had recommended his to her, saying that he had done work for them in the past, so she decided to give him a try. This was when the grooming began.

The handyman told her that both he and his wife worked full time, but that they earned so little money that he did odd jobs and DIY work in his spare time just to make ends meet. Feeling sorry for him, our kind-hearted resident would go out of her way to find jobs for him to do, in order to give him money for his family. Although they were only small jobs, the handyman did not do them very well but charged rather a lot for his work. Our resident overlooked this as she felt sorry for this poor man and his family struggling to make ends meet. The handyman told her numerous tales of hardship, how they sometimes had no money to buy food, so he and his wife would go without food in order to feed their child. So terrible was his situation, that our resident would give him bags of food to take home to his family and at Christmas she bought and cooked a roast that then gave him to take home to his family.

Our resident purchased an e-bike and decided that she would like a shed in her front garden to store it in, so she contacted the handyman. He visited her home and explained how he would lay a concrete base and then construct the shed from plastic cladding, for which he would charge her £3,500 as he would complete the whole job in one day. This seemed rather quick given that the concrete base would need to set and she was unsure as to the sturdiness of the plastic cladding, but as feeling sorry for him, she went along with this and transferred into his bank account the £2,000 deposit that he said he needed to buy the materials. A couple of days later the handyman contacted her and claimed that his wife had gone to a casino and gambled the whole £2,000 away, stating that she has a gambling problem and that is why they have no money. Instead of apologising and offering to make amends to the resident, the handyman started pressuring her to pay him the remaining £1,500 to buy materials for the shed. However, the resident was so alarmed by this that she refused to pay him anymore and instead asked him to build her shed. The handyman made 3 appointments to go to the house and build the shed, but always failed to appear; so the resident asked him to return her £2,000 but he then stopped answering her calls and texts.

Distraught, the resident shared this bad experience with her 'friends' online, they laughed, suggesting that similar things had happened in the past and that the resident would probably get her money back eventually.

In recounting to us what had happened since the handyman had first been recommended to her, the resident saw that she had been taken advantage of, falling for his tales of hardship, buying him food and paying over the odds for his poor-quality work. She also felt let down by her social media friends who had recommended his to her, although they must have known that he was not very good at the work and that she might well lose money to him.

Fortunately, after reporting the incident to her bank and to the police, the handyman did contact her and repaid the whole £2,000. But it was almost a costly lesson and in future she will look for her tradesperson using reputable sources, not 'friends' on social media.

New regulations for consumers regarding protection from unfair trading.

It is a measure of its longevity that references to the Trade Descriptions Act 1968 can still be heard and seen in anything from comedic performances to letters of complaints to the newspapers.

However, it is a fact that from 2008 until 2025, the Consumer Protection from Unfair Trading Regulations 2008 (known as the CPRs) controlled unfair practices used by traders when dealing with consumers, and created criminal offences for traders that breached them.

Expected to become law from 6 April 2025, controls over unfair practices will now be found in the equally snappily named Digital Markets, Competition and Consumers Act 2024 (DMCCA) - “the Act”. In reality, for consumers the Act changes little, but takes the opportunity to make improvements and – as is recognised by its title - to fully recognise the role of the digital market for consumers.

Central to the Act remains the concept of the 'transactional decision’. Simply put this means any decision made by a consumer from deciding whether or not to purchase a product (goods or services); how to purchase it; right through to after sales and for the lifetime of the product.

To assist in the protection of consumers, the Act prohibits trading practices that are considered unfair to consumers. These include misleading actions and omissions; aggressive practices; and creates a general duty not to trade unfairly. Importantly, for these practices, it is necessary to show that the action of the trader is likely to have an effect on the actions of the consumer.

For the purposes of determining this, the Act has created an “average” consumer, one who is considered to be “reasonably well informed, reasonably observant and circumspect”. This is a very important definition and in cases judges have shown that they expect consumers to have at least made some checks when deciding whether to go ahead with a purchase and not to behave irrationally when making decisions.

However, the Act also recognises that some traders effectively act outside the law and so two other categories of consumers have been identified – those where practices are targeted against a particular group of consumers; and also where consumers are vulnerable by means of age, mental health, or other circumstances.

The latter is particularly relevant, for example, in the area of doorstep crime, and in those cases, consumers who are victims of those practices are usually not expected to have fully consented to the works.

The Act also introduces 32 banned practices considered to be unfair to consumers and prohibited in all circumstances. These include everything from the unauthorised use of membership logos to bogus closing down sales, or from pyramid schemes to aggressive sales techniques.

31 of these banned practices were present in the previous CPRs, but one new one has been created covering the use of fake consumer reviews and/or not revealing that the review has been paid for. This practice has in recent years become widespread on social media often led by so called “celebrities”.

Finally, the Act will, in due course, provide consumers with rights of redress in respect of misleading and aggressive commercial practices, and set out the remedies available to them.

Provisions are currently to be found in the CPRs. There are three main remedies available to a consumer: the right to unwind – effectively to undo the contract and return to the position prior to the contract being made: where the contract cannot be unwound, the right to a discount: and the right to compensatory damages.

However, it is fair to say that these provisions have never really been utilised - due largely both to the nature of both the businesses involved and the difficulties faced by consumers in attempting to enforce their rights. Whether the rights of consumers to obtain redress will be easier under the DMCCA will be seen.

Buy Safe, Be Safe: avoid e-bike and e-scooter fires

House fires caused by e-bikes and e-scooters are rising as these products increase in popularity.

In 2023, the London Fire Brigade reported:

93 e-bike house fires (40% of which related to conversions)

18 e-scooter house fires

77% of those involved battery failure. The fires have predominantly been caused by two things:

1. Using a charger that didn't come with the product and isn't produced by the same manufacturer
2. Bike conversions where a home kit has been used

Safely charging your e-bike or e-scooter

- Don’t charge e-bikes and e-scooters in bedrooms or where escape routes can be blocked – for example, hallways.
- Don’t leave your battery charging unattended, when you are out or while you are asleep.
- Don’t cover chargers or battery packs when charging
- Don’t overload sockets or use inappropriate extension leads
- Don’t charge or store batteries in direct sunlight or in hot locations (above 45ºC)
- Don’t charge batteries close to combustible materials or hazardous substances.
- Always unplug your charger when you have finished charging
- If your battery can be removed from your e-bike or e-scooter and charged separately, it should be charged on a hard flat surface where heat can disperse and in area with good ventilation.

For more detailed information about battery safety for your e-cycle or e-scooter, see the guidance published by the Department for Transport:

https://www.gov.uk/government/publications/battery-safety-for-e-cycle-users

https://www.gov.uk/government/publications/battery-safety-for-e-scooter-users

Buying e-bikes and e-scooters

- Only buy e-bikes, e-scooters, chargers and batteries from reputable retailers and manufacturers.
- Check the product is marked with a CE or UKCA mark to ensure they comply with UK product safety standards.
- Check product reviews before buying
- Register your product with the manufacturer to validate any warranties and make it easier for manufacturers to contact you in the event of a safety issue e.g. product recall.
- Check if products have been recalled by visiting the government Product Recalls and Alerts web-site at:

https://www.gov.uk/guidance/product-recalls-and-alerts

Sainsbury's introduce 'lock' to counter wave of Nectar points fraud

Millions of Nectar points have been stolen from Sainsbury's shoppers over the past year.

Sainsbury's has boosted the security of its Nectar points app, in a bid to help protect shoppers being defrauded of their Nectar reward points.

The supermarket began rolling out a new 'Spend Lock' at the start of February. The security feature allows shoppers to freeze their account, and set where their reward points can be redeemed.

Previously there was no lock or limit on where points could be redeemed, meaning that in theory anyone with access to an account holder's barcode or account number could redeem the points.

The lock is one of several security measures Sainsbury's has introduced over recent months after hundreds of Sainsbury's shoppers reported having their accumulated Nectar points stolen.

National newspapers, first reported the issue, in January 2025 that Sainsbury's customers had been defrauded of an estimated 12.5 million rewards points, worth the equivalent of more than £63,000 over the past year, by scammers who had accessed their Nectar accounts.

Newspapers received reports from dozens of shoppers claiming they had been defrauded of their points. Some claimed their rewards had been redeemed in shops hundreds of miles from where they live, despite fraudsters seemingly having no access to their physical card, app or other information.

The supermarket has not revealed how scammers had been able to access such vast amounts of data, claiming that doing so publicly could encourage more scammers. However, it's been reported that criminals have been circulating lists of thousands of anonymous Nectar account numbers via secure messaging apps, with some even selling access to accounts.

Now, if the function is enabled, an account holder will have to give manual permission each time they attempt to redeem points. The lock – which now appears in the app's settings – can only be actioned or disabled by the account holder. However, the lock has still not been fully rolled out to all Nectar accounts.

Digital crime is a growing problem for supermarkets

Nectar points are accumulated each time a shopper scans their card, based on the total amount of the transaction, and can be redeemed with money-off shops in Sainsbury's and Argos or through one of Nectar's recognised partners, which include British Airways and the Woodland Trust.

Fraud and digital security is becoming a growing issue for supermarkets who like Sainsbury's, have been expanding their use of data and digital technology.

Reimbursement Toolkit

The National Trading Standards Scam Team, in conjunction with member banks have created a guide that has been designed to help you to apply to your bank or building society to ask for your money back if you have been the **victim of a fraud** – that is you have been tricked into paying money to **someone (by direct transfer, cheque or cash)** who was not who they said they were or never intended to provide the goods and services that they promised.

Included in the toolkit:
- Quick help sheet
- Template letter to your bank explaining your case
- Your bank's role
- What is the Contingent Reimbursement Model Code?
- After the claim

Call your bank as soon as possible to report that you've been the victim of a fraud.

Most banks have a dedicated phone number to report fraud or scams – you will find this on your bank's website. If you don't have access to the internet, call the number on the back of your card and ask to report a fraud. You can also report fraud to most large banks and building societies by calling 159. If you or someone else is in immediate danger because of a scam (for example, being threatened by an aggressive doorstep caller), call the police on 999.

Report the scam to Action Fraud: visit the website (www.actionfraud.police.uk) or call 0300 123 2040.

You can also get further advice and support by calling Citizens Advice 0808 223 1133 or visit the website (www.citizensadvice.org.uk).

The link to the guide is below:

https://www.friendsagainstscams.org.uk/mint-project/uploads/942501906.pdf – this is a link to a safe PDF file.

Alternatively you can contact Croydon Trading Standards to request a copy of the document to assist you but emailing trading.standards@croydon.gov.uk and asking for the Reimbursement Toolkit.

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**

STOP! THINK FRAUD

METROPOLITAN POLICE

FRAUD!

SPOT IT AND STOP IT!

Calls claiming to be the bank or the police

Sudden claims of suspicious banking activity

Being asked for PIN number or passwords

Requests for bank card or cash as 'evidence'

Asked to purchase high-end jewellery and goods

'Couriers' sent to collect card, cash, or bank details

METROPOLITAN POLICE STOP! THINK FRAUD

MORE TRUST | LESS CRIME | HIGH STANDARDS

KNOW HOW THE FRAUDSTERS WORK...

A FRAUDSTER'S CALL TO YOU
Spot it and stop it!

A criminal contacts you, pretending to be a police officer or bank official. They claim there is an issue with your bank account, or request your assistance with an investigation.

They ask you to withdraw cash or foreign currency, provide your bank cards or PIN numbers, purchase high value items such as gold bullion, or hand over jewellery which will later be collected by a courier from your home.

STOP FRAUD

POLICE OR BANK OFFICIALS WILL NEVER ASK FOR PIN NUMBERS, BANK CARDS, GOODS OR MONEY!

To make sure the caller is from the bank or really a police officer, hang up the phone at the start of the call and wait 5 minutes (criminals stay on your phone line) or use a different phone and call:

101 – to verify if the person is a police officer.

159 – to speak to your bank
(or call the number on back of card).

If you have been a victim of fraud then speak to your bank and report to **ACTION FRAUD** on **0300 123 2040**