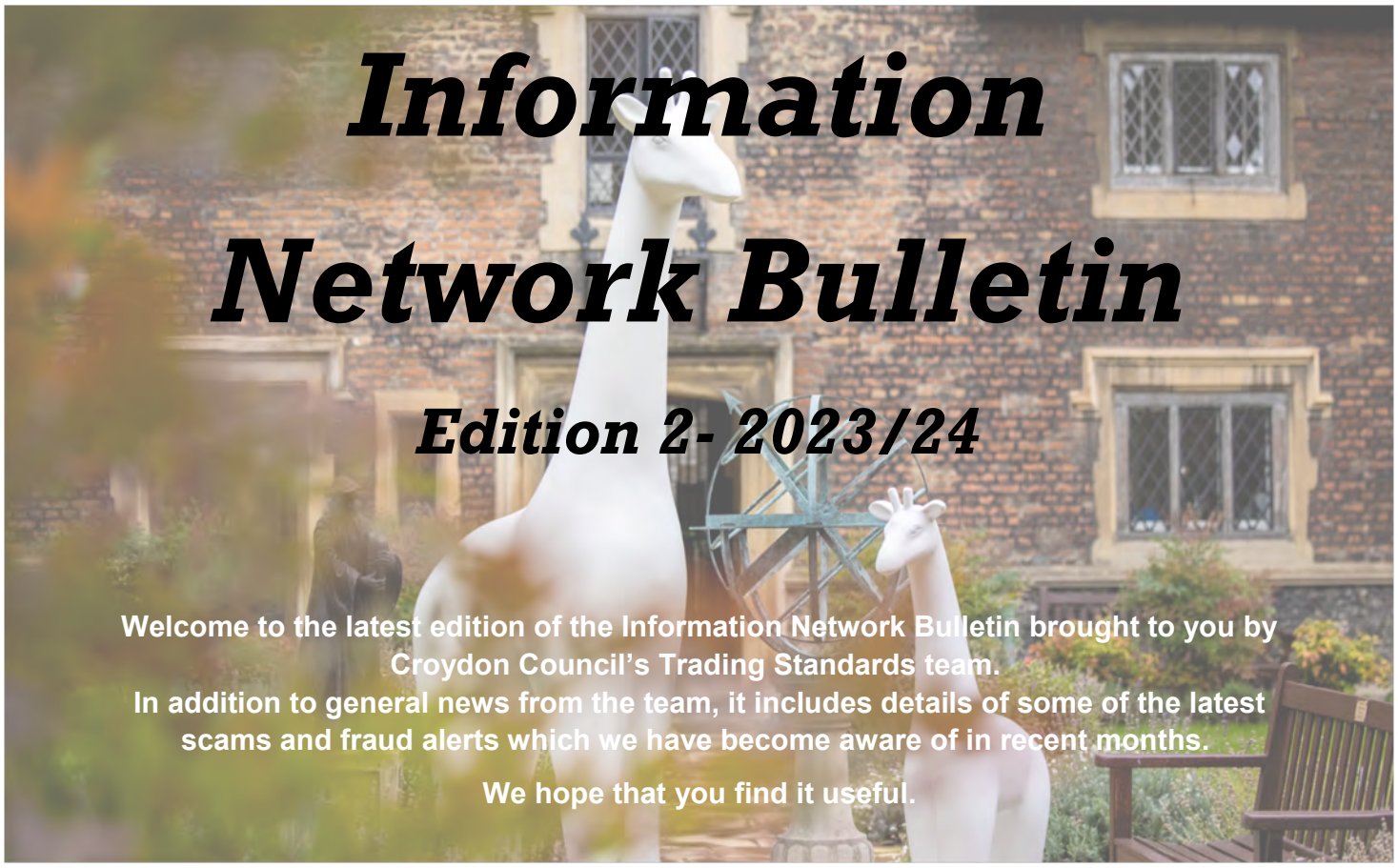

Information Network Bulletin

Edition 2- 2023/24

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.

Student Life

A new academic year sees a new intake of young people living away from home for the first time and controlling their own finances. Here are some tips and warnings for them to be aware of:

Hard luck/lost card scams
This is where you are approached by someone who claims to have lost their bank card and needs money. They ask you for cash and in return they will transfer the money into your account. They are likely to make a payment to you on a fake banking app, meaning no money has gone into your bank account.

Money mules
'Money mules' receive stolen funds into their account and are then asked to withdraw and wire the money to a different account (often overseas), keeping some of the money for themselves.
Even if you are unaware that the money you are transferring was illegally obtained, you can still be prosecuted for money laundering.
Remember, you should never give your financial details to someone you don't know and trust.

Bank account at risk
This is where you receive a call or text telling you your bank account has been attacked and for safety reasons your money will need to be moved into a new account.
Banks will never call you to ask you to move your money. Hang up and call your bank from the number on the back of your card or you can contact most bank fraud lines by calling 159.

Fake refunds or unexpected windfall
You receive a text message or email from a company (usually Amazon, HMRC or Royal Mail) saying that you are owed money and asking for your bank account details to process the refund. Do not respond to the email or text. Go to the company's website to verify the refund is legitimate.

Student Loans Company Phishing Scam
You receive an email or Text from what appears to be the student loan company asking for bank details. Do not follow a link in the message but search the official company page and ensure you are on the official web page.

How to Spot a Fake Website

It can be difficult to spot a fake, fraudulent or scam website. With Christmas coming up, and many of us turning to online shopping, we recommend you follow Which? Consumer magazine's eight simple tips below to test whether a website is legitimate or not.

1. Double-check the domain name
Many fraudulent websites use a domain name that references a well-known brand or product name. For example, website domains such as www.ipadoffers.net or www.discountnikeclothes.com should raise alarm bells. You should also be cautious of domains that end in .net or .org. These are rarely used for online shopping so may have been acquired by questionable people or organisations.

2. Is the offer too good to be true?
If prices seem too good to be true then, sadly, they probably are. Scam websites use low prices to lure bargain-hungry shoppers in order to quickly sell fake, counterfeit or non-existent items.

3. Never pay by bank transfer
If you are asked to pay for something online via a bank transfer, don't do it.
If you buy an item that turns out to be fake or non-existent with a credit or debit card, you do have some rights to get your money back.

4. Browse the website
Watch out for poor English, such as spelling and grammar mistakes, or phrases that don't sound quite right. Keep an eye out for pixelated images or graphics, and out-of-date logos or branding. You should also check that the website lists contact information. Legitimate companies will always list how to get in touch with them; if the website doesn't have a 'Contact us' page with address, phone and email, it could well be fraudulent. If the site does have 'Contact us' page but only offers a form to fill out, be wary as this could also be an indication of a dubious website. If none of this information is available, you should treat the website as highly suspicious.

5. Check the returns policy
If the company is selling a product online, it should have a shipping and returns policy listed on its website. If it's a real company, it should tell you how and where to return a faulty item.
The website should also have terms and conditions, and a privacy policy that tells you exactly what it plans to do with any data you share and any extra contractual rights you may have. Check these apply to the country you are in. Often scammers use cut and paste T&Cs from websites based abroad.

6. Read online reviews
Look at reviews across a number of sources, such as Trustpilot, Feefo or Sitejabber, which aggregate customer reviews. Note that all positive reviews, or blocks of positive reviews dated close together or very recently may indicate fake reviews. You should also check the company's social media pages for recent activity and to see what other people are posting on their social channels

7. Can you trust a trust mark?
Research carried out by ANEC, a European consumer organisation, found that seven in ten people say they're more likely to use a website with a trust-mark label or logo.
However, just because a website appears to carry the logo of a reputable trade organisation, it still doesn't necessarily mean the website is genuine. If you're in doubt, you should always contact the trust-mark company to check. You can often check membership by checking their website.

8. Look for a padlock
A padlock next to a website's URL means the site is encrypted, so what you do on it – such as browse or make payments – can't be intercepted. Most websites now have this feature, so if you notice a site doesn't have one it could be a red flag. But equally, scammers are able to forge or buy these padlocks, so seeing one doesn't always mean a website is safe.
Looking for a padlock should always be combined with the other checks we've recommended.

Croydon Underage Sale Prosecution

A business in Thornton Heath has been fined for selling a vape to a person under the age of 18, as Croydon Council's trading standards service cracks down on illegal sales to minors.

The council's trading standards service has been helping to keep Croydon's young people safe by carrying out enforcement action on the illegal sales of goods to those underage – including knives, alcohol and vapes.

As part of this activity, the team worked with a volunteer teenager to carry out a test purchase of a Bloody Mary 'Mr Blue' vape at P&N Convenience Store in Bensham Lane, Thornton Heath.

The council's underage volunteer gave her correct age of 15 on request from the seller twice, however the transaction proceeded.

At a hearing at Croydon Magistrates' Court on Monday 21 August, A&AK Patel Ltd – the trading name of the store – admitted carrying out the sale of a vape to a minor.

The court heard that, despite a warning notice on display in the shop window saying vapes would only be sold to people aged 18 and over, the sale was made. Enforcement officers also found that no written records had been kept confirming employees had been trained about underage sales, and there was no till prompt system in place to help remind staff.

A&AK Patel Ltd was ordered to pay a £920 fine, £910.80 in costs and a £372 victim surcharge, totalling £2,202.

"Making the borough safer for our young people is a top priority for me and I am determined to protect young people from the illegal sales of vapes, alcohol and knives.

"Our trading standards service work closely with local businesses to ensure they are up to date with the latest legislation but, where sellers flout the law, we will not hesitate to take enforcement action to help keep Croydon's residents safe."

Jason Perry, Executive Mayor of Croydon

Croydon Trading Standards Need Test Purchasers

Trading Standards work with young people to monitor the sales of age-restricted products across Croydon. Part of this work involves a young person under strictly controlled conditions trying to buy knives, alcohol, fireworks and cigarettes & vapes from shops in the borough. We are looking for volunteers, aged between 14-16 years and 18-24 years to help us carry out test purchasing activities.

To find out more and sign up as a test purchaser contact Croydon Trading Standards by email at:
trading.standards@croydon.gov.uk
or call us on 020 8407 1311

Buying a Used Car

Although in many ways the second hand car market has been revolutionised by the rise in the number of online vehicle sellers which give consumers 14 days to properly examine the vehicle, the used car industry is still one of the most complained about sectors.

However, it is important that consumers manage their expectations when purchasing a vehicle at the lower end of the market. For some time now, the increasingly high prices of new vehicles has also meant that used car prices remain high and cars well over ten years old may cost amounts in the low thousands.

This may well be exacerbated by the introduction of the expansion of ULEZ as consumers seek to exchange their non-compliant vehicles and which may have a further effect on the cost of used vehicles. (You can check the ULEZ compliance of a car which you wish to purchase at https://ulez.co.uk/ulez-checker/)

When purchasing a used car, a consumer is entitled to expect a car of satisfactory quality. Satisfactory quality means that the vehicle you purchase should be of a standard that a reasonable person would expect, taking into account a number of factors including the vehicle's history, age and value

An old car with a high mileage cannot be expected to be as good as a newer car with lower mileage, but should still be fit for the road. Similarly, it is likely that an older car will have minor defects in appearance and finish, and wear and tear must be expected reflecting its age.

However, a consumer who purchases a vehicle sold with a minor defect which is present at the point of sale and renders a vehicle dangerous or leads to a catastrophic failure - effectively meaning that the vehicle cannot be economically repaired - would be entitled to compensation.

Should this occur in the first thirty days after purchase, a consumer is entitled to a full refund. If an issue arises after this date, you may still have rights which you can read at –

https://www.croydon.gov.uk/business-licences-and-tenders/trading-standards/trading-standards-consumer-advice-and-guidelines/consumer-advice-goods-services-and-safety-recalls/advice-and-support-citizens-advice

If you feel that a used car business is trying to restrict your rights prior to or after you purchase a vehicle, you should initially call for full civil advice the Citizens Advice Consumer Service (CACS) on 0808 223 1133.

If CACS believe there may be issues for Trading Standards they will refer the matter to ourselves and we may be in contact with you.

Your Rights Following Disruption to Flights from UK Airports

Following the flight disruption in UK airports earlier this Summer, here is some advice to travellers about their rights.

I'm stranded in the airport

The law requires airlines to offer assistance to passengers who find themselves stranded in an airport due to flight disruption. You should be offered reasonable non-alcoholic refreshments, accommodation (if a replacement flight requires an overnight stay) and transport between the airport and your accommodation.

The point at which you are entitled to this assistance depends on the length of the delay and distance of your flight. For flights of less than 1,500km, the rights accrue after a delay of two hours or more, three hours or more for flights between 1,500 and 3,500km, and a delay of four hours for all other flights.

If the new expected departure time is at least the day after the initially scheduled departure time, you are entitled to accommodation and transport to and from the airport and your accommodation.

Flight cancellations and delays

If your flight was cancelled, and the airline is based within the European Union or was departing from the UK, there is a legal right to a choice between being put on another flight to your destination or getting a refund of the value of your unused flight ticket. You can only choose one of these options.

In a situation where the cause of the cancellation or delay is a more general issue, impacting all airlines, you may have to wait for an alternative route, which might impact on other bookings you have such as hotels.

Compensation

Additional compensation to the above rights is only available where the reason for cancellation was within the control of the airline - this is unlikely with a general air traffic problem.

Impact on other services such as hotel bookings

If you booked your flight as part of a package covering other travel services like accommodation, you might have rights through your package travel organiser, so contacting them for a solution can also be helpful.

If you have booked holiday or travel services separately through different providers, you may not have a right to cancel such items as hotel bookings if you can't get to the hotel on the specified day. You may also not have a right to change the dates of the booking. Of course, you should contact the service provider as early as possible and let them know of the problems you are facing, to see if they might be willing to adjust your arrangements.

You may however need to make new arrangements yourself, at your own cost.

If you have holiday insurance you should let your insurer know as soon as possible as this may be the only avenue available for compensation.

Make contact with the airline or your package travel organiser to outline your complaint and tell them what you would like them to do to put the problem right. Formal complaints communicated in writing can have more impact than a telephone call and can often result in a positive solution to a complaint. We recommend that you allow them a reasonable amount of time in which to respond (around three weeks) and if your case is still unresolved after having made contact with them, you can get in touch with UKICC (UK International Consumer Centre) who might be able to offer further help.

We also advise you to contact the bank/credit card company you used to pay for your holiday as they may also be able to help you claim if your claim is about a refund of the unused ticket.

Parking

Scams are on the rise with criminals finding ever more devious ways to scam people. The last year has seen a rise in parking scams.

The first type of scam involves scammers placing their own QR code over the genuine ones on display in carparks.

People scan the code and enter their credit card information thinking they are paying for the space, but instead, it directs them to a fake website where scammers capture their payment details and take larger sums of money as well as capturing personal details which could be later used in fraud. Some people are finding they have signed up for subscription services which do not exist but take money every month.

Fake posters and signs are also being put up and taken down periodically which mimic the genuine companies and ensures people are duped and diverted to fake websites or apps. Due to not actually having paid for the space, people are also receiving parking tickets too.

We urge consumers to exercise caution when providing their credit or debit card details online by ensuring the website being used are genuine.

To avoid these scams, ensure you only download parking apps directly through the App Store or official app provider, typing the official website directly into your browser or calling the phone number associated with the company.

Do not use the QR codes displayed and search for the official company online, do not rely on the website given on a poster.

Ensure you check your bank account regularly and challenge suspicious payments that you cannot account for. If you find you have been the victim of a scam, speak to your bank to be advised on what steps to take and report the crime to Action Fraud at www.actionfraud.police.uk or call an advisor on 0300 123 2040.

ActionFraud
National Fraud & Cyber Crime Reporting Centre
0300 123 2040

Fraudsters Target WhatsApp Users

WhatsApp users, especially those part of religious and community groups, are being deceived into sending money to scammers.

The fraudsters ring their victims, posing as members of the group - to help gain trust. They will use a fake profile photo and name, to add to sound more believable. The thieves then say they're sending a one-time passcode which will allegedly allow the victim to join an upcoming call for all members. The scammer then asks the victim to share this passcode with them so they can be "registered" for the video call. But in reality, the scammers are asking for a registration code to register the victim's WhatsApp account to a new device where they then transfer their WhatsApp profile over.

Once in the victim's profile, the fraudsters enable the two-step verification, locking the user out of their account. The fraudsters, posing as the victim, then send messages to other group members asking them for money, relying on the goodwill of group members and their intrinsic desire to help others in distress.

Croydon Trading Standards warn: "WhatsApp continues to be a popular platform for community and religious groups, but sadly also for fraudsters. We urge people always to be wary when receiving contact via WhatsApp or other messaging platforms. This is particularly the case when being asked to provide account information – despite the fact that you may recognise the individual's profile picture and / or name."

Trading Standards advise: "Never share your account information with anyone, and if you think it's a fraudulent approach, report the message and block the sender within WhatsApp. To make your account more secure, we advise setting up two-step verification to provide an extra layer of protection. This makes it increasingly more difficult for fraudsters to gain access to somebody else's WhatsApp account."

How to avoid the scam:

1. Never sharing your account's two-factor authentication code.
2. Setting up two-step verification provides extra security. To do this, open WhatsApp settings, tap account and choose two-step verification then 'enable'.
3. If a message from a friend or family member is asking for money on WhatsApp, call them to double-check.
4. Finally, you can report a message and block the sender on WhatsApp.

Remember, if you have been a victim of fraud or cybercrime, report it at www.actionfraud.police.uk or by calling 0300 123 2040.

Illegal Tobacco Reminder

Croydon Trading Standards are continuing their work on eliminating illegal tobacco from the borough. Illegal tobacco supports criminals and organised crime.
If you are aware of any shops or market traders 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, or any traders selling singles, please report them 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 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/

Call 159

STOP
HANG UP
CALL 159

If you think someone is trying to trick you into handing over money or personal details - stop, hang up and call 159 to speak directly to your bank.

Stop Scams UK is an industry-led collaboration of responsible businesses from across the banking, telecoms and technology sectors who have come together to help stop scams at source. They have collaborated to enable and facilitate the development of technical solutions that will help prevent the harm and loss caused by scams.

Almost all scams will touch on two or more of the banking, technology and telecoms sectors. The work of Stop Scams UK in bringing business from across these three key sectors together is crucial in creating the holistic, systemic solutions necessary to keep all of us safe.

How it works

159 works in the same way as 101 for the police or 111 for the NHS. It's the number you can trust to get you through to your bank safely and securely, every time. So if you think someone is trying to trick you into handing over money or personal details - stop, hang up and call 159 to speak directly to your bank.

What does it cost?

The cost of calling 159 will vary according to your phone provider. In many cases this will be the same as a national rate call. Please ask your provider for details.

Who can use 159?

The banks that currently use 159 are:

Barclays
Bank of Scotland
Co-operative Bank
First Direct
Halifax
HSBC
Lloyds
Metro Bank
Nationwide Building Society
NatWest
Royal Bank of Scotland
Santander
Starling Bank
Tide
TSB
Ulster Bank

The telephone companies involved in 159 are:

BT (including EE and Plusnet)
Gamma
O2 (including giffgaff)
Sky
TalkTalk
Three
Virgin Media
Vodafone

If you think someone is trying to trick you into handing over money or personal details on the phone - stop, hang up and call 159 to speak directly to your bank for advice.

Investment Scams Increase on Social Media

Investment scams are traditionally known as **boiler room fraud** due to the intense, high pressured sales techniques used to convince you to invest in worthless and or non existent shares. But Croydon Trading standards are receiving increasing numbers of reports from persons being approached on social media to make investments.

Contact is usually made out of the blue by an individual who appears professional and may offer investments in a variety of commodities such as land purchase, crypto currency, carbon credits or vintage wine to name a few. The share offer is supposed to provide the investor an excellent return in a short time frame.

On social media, 'friends' share links to websites claiming that they have made incredible returns in a very short time. Residents have reported being bombarded by messages from new 'friends', all with links to various of these investment sites

One resident even reported being put in touch with someone who was running a pyramid investment scheme on social media. Incredibly, people were actually paying this person money each week with the promise that each month a name would be drawn and receive a few thousand pounds. They reported the scam when they won, but only received a quarter of the money they had expected. In reality, they were lucky to have received anything at all.

The warning signs are:

- unsolicited or cold calls or approaches through social media
- a persistent sales technique
- limited-time only offers giving you no time to consider the nature of the investment
- company names which sound very familiar or have a slight variation to a legitimate company
- secrecy of your investment is encouraged to ensure maximum returns
- issue of false share certificates, research reports or other documentation to make the investments seem credible
- professional looking websites in order to make their business appear legitimate.

Please remember that most of these investments involve unregulated markets, so your investments are not protected. Dealing with an investment criminal will almost certainly result in you losing your money.

If you have been a victim of an investment scam, report it at www.actionfraud.police.uk or by calling 0300 123 2040.

Are you feeling lucky?

As you read this piece, many households across the borough will be receiving “good news” in the form of money won in a lottery, or prize draw.

You’re told via email or letter that you have won a large amount of money on an overseas or online lottery. Spanish, Canadian and Australian lotteries are among the most common.

So that you can process the payment of your winnings, it asks you to contact someone who claims to be an official at the lottery company. You are warned to keep your good luck a secret and, if you don’t respond quickly, you won’t be able to claim your winnings.

After the initial excitement, your first thought should be - how have I won something in a competition which I have never entered and your next action should be to dispose of the letter or delete the email.

It can take a lot of courage to dispose of such a communication. You may ask yourself what if this is actually genuine and what if I am throwing away a large sum of money with which I could perhaps help out family and friends.

The fraudsters who have sent you this letter or email, are counting on you having those thoughts. Many people are suspicious but make the initial response thinking that one call will not hurt.

If you respond to the fraudster, you’ll be asked to supply personal information and copies of official documents, such as your passport, as proof of identity. The fraudsters can then use this information to steal your identity.

The fraudsters may ask for your bank details, saying they will pay your winnings directly into your bank account but if you hand over your bank details, the fraudsters will use them to empty your account. Alternatively, you may be asked to set up a separate bank account for the money to be paid in.

Once you are in communication with these people you will be asked to pay sums of money, usually small at first, to cover so-called legal or banking fees to allow the money to be released. Each time you make a payment, there will be another reason given for delays in paying you and requests for further sums of money to expedite matters.

Be aware that you’re now likely to be a target for other frauds. Fraudsters often share details about people they have successfully targeted or approached, using different identities to commit further frauds.

So, remember if you receive any of this form of communication – recycle or delete!

Further advice can be obtained by emailing trading.standards@croydon.gov.uk

To report a suspected crime, or if you have fallen victim to fraud or cyber-crime, contact Action Fraud via its website or by calling 0300 123 2040

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**