**ISSUE 16** 



Latest news from Redcar & Cleveland Council's STOP COLD CALLING TEAM



# BE VIGILANT – REDCAR & CLEVELAND RESIDENTS TARGETED BY DOORSTEP COLD CALLERS

Unsuspecting householders in our area have been visited by a variety of cold callers in recent months.

Services offered have included driveway cleaning, roofing work, pest control, driveway installation and double-glazing installation.

Some incidents have involved the sale of goods including fish and household/cleaning products.

In one incident a householder answered his door to find two males on his doorstep, (an adult and child), offering household products for sale. The householder declined to make a purchase even telling the caller that there was no money in the house. The caller said that the lack of cash was not a problem as he had a card reader.

The older male said that he had done time in prison, wanted to sort his life out and be a role model to his younger brother.

These types of sellers, known as "Nottingham Knockers", as the scam is believed to have originated in Nottingham, are often young men claiming to be exoffenders or ex-servicemen, call door to door offering a selection of household products for sale from a holdall they carry with them.

The sellers are driven to an area by the person who employs them and given a list of streets to work. The price of the goods is inflated, and they are usually of poor quality. Sellers can be very persistent and occasionally confrontational.

Very often the main purpose of the call is to check out properties and assess the potential for further criminality. This information is then sold on to rogue traders and others involved in criminal activity.

The use of card readers is a new development, the use of which puts the householder at risk of further financial loss. Householders may unwittingly pay a higher price than that quoted when presented with a card reader. Only when they receive their bank statements do they realise that the seller has entered a higher price into the card reader.



# NEW PROPOSALS TO TACKLE FRAUD

New proposals recently announced by the government include prevention measures, an improved reporting system, support and justice for victims and an improved response to fraud by enforcement agencies.

#### PREVENTION:

- Cold calling to sell financial products, including cryptocurrency will be banned. This will prevent fraudsters from selling fake investments.
- Sim Farms will be banned. A sim farm is where a large number of sim cards are used to send out thousands of scam messages at once.
- A clampdown on number spoofing by working with OFCOM to make it harder for fraudsters to make it look as though they are calling from legitimate businesses.
- A review of mass text aggregators will be undertaken with a view to stopping fraudsters from sending scam texts in bulk messages.
- Make the technology sector put extra protections in place.

### **REPORTING:**

 Action Fraud will be replaced with a new system for the reporting of fraud and cyber-crime. The system will allow anyone reporting a crime to track the progress of their report and receive updates.

### **VICTIM SUPPORT:**

- Ensure clear messaging on how the public can protect itself from fraud and how to report it.
- Change the law to ensure victims will get their money back.

### **ENFORCEMENT:**

- Introduce a new national fraud squad.
- Take the lead in a new global partnership to pursue fraudsters wherever they are based.

In addition to these measures, Anthony Browne MP will be appointed as a new antifraud champion and banks will be allowed to delay the processing of payments so suspicious payments can be investigated. This will help protect anyone falling victim to authorised push payment fraud where a person is tricked into sending money to a fraudster who is posing as a genuine payee.

### **SCAM ALERT**

# The "Hi Mum" or "Family Emergency" scam



This is a scam that many are familiar with now. In its original form parents receive a message purporting to come from a teenage child asking for urgent financial assistance. The text or WhatsApp message is sent by scammers and simply states that their phone has been lost or damaged and they need money to buy a new one.

As awareness about the scam has increased it has become less successful, so fraudsters have developed it so that messages can go on for days. Messages include a lot of personal information harvested from social media accounts and kisses are put in the messages.



In a variation of the scam messages are also sent to elderly parents by scammers purporting to be an adult child. In one version of this type of scam the parent receives a message from an adult child telling them that they have lost or damaged their phone so they cannot access online banking and they have an urgent bill to pay so can the parent transfer cash to a friend's account.

Scammers have also reversed the scam so that messages purport to come from elderly parents to their adult children requesting money due to an urgent situation that has arisen, for example a forgotten purse while out shopping.

On receipt of any messages that put you in the situation where you feel the need to respond immediately the advice is to stay calm and not react to the urgency of the situation presented or the emotional language used.

Try to contact the family member or a friend using a known number or email address and ask if they have contacted you. Be wary of any response which comes from a different phone number or email.

If you are not convinced that the request is genuine do not send any money.

#### **QR Code scams**



Quick Response (QR) codes are turning into an easy way for fraudsters to collect personal information and take money from your bank account.

These codes allow you to access websites to pay for goods and services.

Unfortunately, fraudsters have started sticking these codes over legitimate ones on parking meters, menus, and electric charging points so when you use the code you are directed to a fake website which requests bank details for a payment. This is known as QR code jacking.

Fraudsters also include QR codes on fake delivery notes for parcels they claim they haven't been able to deliver. You are asked to scan the QR code on the note, which has been pushed through your letter box, to reschedule delivery.

Finally, you may also receive a "Quishing" email. This is an email which contains a QR code purporting to come from a trusted organisation such as a bank or HMRC. You are encouraged to use the QR code, but it takes you to a fake website through which they take money from you or harvest personal information.

One such scam takes place when the fraudsters pretend to be from a bank and say that they are improving security by upgrading to QR codes and away from two factor authentication. You are asked for passwords and banking information which the fraudsters use to log on to the account and steal your money.

- Be cautious when using QR codes in a public place. Take a close look to see if there are any signs it has been placed over another QR code.
- Check QR codes for any misspelling or graphics that are of poor quality.
- Double check that a website you are directed to is genuine – look at the URL and check that it is valid or ask a staff member if one is present.



 Make sure that the website starts "https". If in doubt, then close the website and access it directly by typing in the website address.

### **Loan Scams**



Loan fee fraud is an increasingly common scam, where people as asked to pay an upfront fee but then never receive the loan.

Pressure will be put on you to pay the fee quickly, often by bank transfer or sometimes using a voucher from Amazon or eBay. You may even be told that the fee is refundable.

The Financial Conduct Authority provides the following advice:

If you need to apply for a loan, you should only deal with authorised firms. If you don't, you won't be protected if things go wrong, and you could end up losing lots of money.

- Check our <u>Financial Services</u> <u>Register</u> to find out if the firm is authorised.
- Check that the firm's contact details match the details on the FS Register.
- Always use the contact details on the FS Register, rather than a direct line or email you've been given.
- If there are no contact details on the FS Register, or the firm claims they are out of date, call us on 0800 111 6768.

### **Puppy Rehoming scam**



The dog rescue and rehoming charity, Dogs Trust and the Chartered Trading Standards Institute have teamed up to warn the public about scammers who are charging money up front for puppies that will never be provided.

The scam starts with a post on social media, "Kelly staffy puppies for sale". The scammers ask for money and personal information. Victims are given the Dogs Trust Leeds Rehoming Centre as the address to collect the puppies from but are left heartbroken and out of pocket when they get there and find that they have been deceived.

Dogs Trust offers the following advice:

When buying a puppy, do your research first, and if something doesn't feel right, don't do it. If an advert seems too good to be true, it probably is. Never pay for a puppy upfront, and always go to see the mother with the puppies, visiting multiple times before you commit.

Ask to see vaccination records; any legitimate breeder would be happy for you to come and see the dog with its mother and give that kind of information. And no legitimate breeder would ever ask you to pay for an animal's vets bills before you buy it.

For more information about this scam visit: <a href="https://www.tradingstandards.uk">https://www.tradingstandards.uk</a>



### **COURIER FRAUD**

Silver pound swindlers: UK's senior population lose more than £12.6 million in the last year to courier fraudsters.

People over the age of 70 are being disproportionately targeted by courier fraud, new data from the City of London Police reveals.

Data from the National Fraud Intelligence Bureau, run by the City of London Police, the national lead force for fraud, revealed that people in their 70s or older lost more than £12.6 million to courier fraud last year, 77 per cent of all money stolen by this type of fraud.

The split of fraud reports made by men and women aged 70 or above was 37 per cent and 63 per cent. Shockingly, data shows 153 reports were made by people in their 90s with one report being from someone aged over 100.

In the last year (May 2022 to May 2023), 1,587 reports of courier fraud were made by people over the age of 70 across the UK. A total of 1,847 reports of courier fraud were made.

The top areas, where 43 per cent of all reports were received from victims, were the Metropolitan, Surrey, Sussex, Thames Valley and Hampshire police areas. In the last year, a total of £16.3 million was lost to courier fraud.

Reports to Action Fraud, also run by the City of London Police, identified a link of courier fraudsters targeting locations such as retirement homes and villages, care homes and buildings that provided assisted living, often targeting some of the country's most vulnerable and oldest members of society.

Detective Chief Inspector Lee Parish, from the Fraud Operations team at City of London Police, says:

"Courier fraud is a devastating crime that preys on vulnerable and often older people. Millions of pounds of hard-earned pensions and savings are being stolen each year and we are concentrating efforts to stop courier fraud at the source.

"We've seen a growing trend of courier fraud taking place in and around retirement villages, care homes and assisted living accommodation. We're asking family members and staff supporting older people across the UK to be vigilant, especially for incoming phone calls to residents, couriers arriving by motorbike or taxi and to any visitors who unexpectedly arrive.

"Banks or police officers will never send a courier to pick up cash, bank cards or pin codes from individuals and we would encourage anyone who thinks they are being targeted to report it using Action Fraud and also separately report it to their bank. If there is a crime currently taking place, you should always call 999."

The City of London Police led an intensification period on operational activity to target those who commit courier fraud. Additional resources were used, facilitated by City of London Police, to scale up both existing and new investigations that resulted in multiple warrants executed across the country.

### What is courier fraud?

Courier fraud is a sophisticated scam that preys on the trust and vulnerability of individuals. The perpetrators often employ cunning tactics to deceive victims into believing they are assisting the police or employees from their bank. This type of fraud typically begins with a phone call or email, where the fraudsters pose as bank officials, police officers, or other authority figures.

Once they establish contact, the fraudsters manipulate their victims with convincing stories, often claiming that there has been fraudulent activity on their bank accounts.



They will try to create a sense of urgency and coerce the victims into complying with their demands.

One common tactic in courier fraud involves convincing victims to withdraw large sums of money from their bank accounts. The fraudsters instruct the victims to place the cash in an envelope or bag and hand it over to a courier who will visit their home to collect it.

Courier fraudsters have also been known to coerce victims in to using mini cabs and taxi services where they are then sent to jewellers to purchase high-value items. Reports have also shown that victims have been sent to foreign exchange bureaus, where they are instructed to electronically transfer money for "safe-keeping".

Another variation of courier fraud involves convincing victims to hand over their bank cards, PIN numbers, or other sensitive information such as answers to security questions. The fraudsters claim that they need these details to verify the legitimacy of the victim's account or to assist in their investigation. Once the victims disclose this information, the fraudsters gain access to their funds and can carry out unauthorised transactions.

### To stay safe and protect yourself, remember:

- Your bank or the police will never call and ask you to verify your personal details or PIN. If you get a call asking you to do this, hang up, wait a few minutes and call your bank on a number you know to be genuine, such as the one on the back of your card.
- Your bank or the police will never send a courier to your home to collect your cash, bank cards, PINs, or any other

### valuable goods. Any requests to do so are part of a scam.

Remember, staying cautious and sceptical can go a long way in protecting yourself from courier fraud. Take the time to verify information, seek advice from trusted sources, and never rush into making financial decisions under pressure.

If you think you've been a victim of fraud, contact your bank immediately and report it to Action Fraud online at <a href="actionfraud.police.uk">actionfraud.police.uk</a> or by calling 0300 123 2040, or call Police Scotland on 101.

# SPOTLIGHT ON HOLIDAY SCAMS



Action Fraud has recently reported that in the last financial year it received 6547 reports of holiday fraud with victims losing over £15m.

Don't get caught out.

#### 5 Common scams:

 Invoice fraud – criminals hack into the emails of holiday company's customers, monitor the email exchanges and when payment for the holiday is due, they insert themselves into the email thread, provide their bank details and take the money. Their email and the customer's reply are deleted before the holiday company can see them.



- Cloned airline and holiday websites

   criminals change the URL of a trusted website, so it appears that you are on a genuine website.
   Some holidaymakers only find out that their holiday does not exist when they turn up to the property they have booked or the airport for check in.
- Fake websites offering available properties or flights at very low prices – fraudsters set up fake websites offering extremely good deals, but the holiday or flights do not exist and victims lose their money.
- 4. Comparison site scam fraudsters tempt customers away from legitimate booking or comparison websites with adverts, offering a better deal on the accommodation or flights about to be booked. These adverts are embedded in the website or can appear as pop ups. Payment is usually requested by bank transfer, or fraudsters may contact the customer direct asking for bank details. By the time victims realise that they have been deceived it is too late as money has already changed hands.
- 5. Free holiday scam fraudsters make contact by email, phone, social media, or text stating that you have won a free holiday but to get the holiday an administration fee is payable. Not only can victims lose money fraudsters can also use their bank accounts for further financial gain.

Get Safe Online offers the following advice:

 Always do your research into accommodation, flights, cruises, package holidays or pilgrimages to check they're authentic. This should include whether it's a package holiday, where two or more travel services (e.g. flight, accommodation and car hire) are combined. Legitimate package holidays should ensure your money is protected and that the online travel agent or tour operator takes responsibility for all their suppliers.

When booking a flight-inclusive package, ensure that the holiday is protected by an ATOL, which ensures your money is safe.

- **Be wary** of unusually cheap holidays/flights or high deposits.
- Confirm that accommodation really exists by finding it on Google Maps and looking for independent reviews and recommendations. If you can, call and speak to the owner/agent directly to try to ascertain if the person you're booking the holiday with is authorised to sell it to you. If the number is not provided, email and request it. Ask questions to see if they have knowledge of the area.
- Check reviews on TripAdvisor or similar sites.
- If you're booking
   accommodation via
   Airbnb, always keep
   communications and payment on
   the Airbnb platform, and don't be
   tempted off it as this may indicate
   an attempt at fraud. Read <u>Airbnb's</u>
   safety advice for guests.
- Never pay for holidays or travel by bank transfer to a company or person you haven't had personal experience of buying from previously. If you do and it's a fraud, you may never get your money back. Paying by credit card means more chance of



getting your money back if something goes wrong.

- Make sure travel agents and tour operators you book holidays and travel through are members of trade associations such as ABTA or ATOL, by checking on these bodies' websites.
- Check terms and conditions prior to making any payment.
- Before paying online or providing any confidential details, type in the website address you know to be correct (instead of following a link) and ensure the payment page is secure (begins with 'https' and has a locked padlock in the browser window frame).
- Keep confirmations and payment receipts, and check bank / credit card statements for irregular entries.
- If you've lost money to fraud, always report it immediately to your bank, as this will increase your chance of getting your money back and the fraudster being traced. Also report it to Action Fraud, the UK's national fraud and cybercrime reporting centre, on 0300 123 20 40 or

at www.actionfraud.police.uk.

### VIDEO – HOW TO AVOID HOLIDAY SCAMS

The Association of British Travel Agents and Kent County Council Trading Standards Service have produced a video for consumers on how to avoid travel related fraud.



Visit: <a href="https://www.abta.com">https://www.abta.com</a> and look at ABTA's tips and Advice page to view the video.

### TRADING STANDARDS NEWS

### ELECTRIC BLANKET & PORTABLE HEATER TESTING



In February this year residents were invited to bring their electric blankets and portable heaters to trading standards for safety testing.

This followed a project in September 2022 when 59% of blankets failed safety testing carried out by GEMS (SW) Ltd.

The blankets and heaters were again tested by Clive McDonald, Managing Director of GEMS (SW) Ltd. 84% of electric blankets failed safety testing and 100% of portable heaters were found to be unsafe.

Two blankets, still in use, had been subject to a manufacturer's recall 25 years ago due to being a fire risk.



Faults found with other blankets included elements overlapping and a power cord down to single insulation.



Electric blanket that failed testing

One portable heater failed due to a broken element with others failing due to their condition and a lack of, or poor, safety features.

Replacements were provided free of charge by trading standards to all residents whose blankets or heaters were found to be unsafe.

The project will take place again on 25<sup>th</sup> and 26<sup>th</sup> of September 2023. Venues will be confirmed closer to the date. However, if would like to register an interest in having your electric blanket tested then contact:

Redcar & Cleveland Trading Standards on 01287 612489 or email tradingstandards@redcar-cleveland.gov.uk

We will take your name and contact details and as soon as the venues are confirmed we will contact you and book an appointment.

### PRODUCT ALERT, REPORTS AND RECALLS

Information on alerts and recalls in relation to consumer products can be found at <a href="https://www.gov.uk/guidance/product-recalls-and-alerts">https://www.gov.uk/guidance/product-recalls-and-alerts</a>

If you want to report an unsafe product or receive advice on your consumer rights, contact the Citizens Advice consumer service helpline on 0808 223 1133. Visit "contact the consumer helpline" at <a href="https://www.citizensadvice.org">https://www.citizensadvice.org</a> for full contact information including webchat and webform.

### **REGISTER YOUR APPLIANCE**

Logging your white goods on the "Register My Appliance" portal means that you can be contacted swiftly if your product is subject to a recall. You will need the following information to register the appliance:

- Brand
- Model name/number
- Serial number
- Purchase date (if this isn't known, an approximate date will do)

The portal, designed by the Association of Manufacturers of Domestic Appliances, can be used to register both new and old goods and can be found at:

https://registermyappliance.org.uk

### **ILLICIT VAPES**

Nicotine-inhaling devices, or 'vapes', have become incredibly popular in recent years and are used by a wide array of people – it is estimated that between 3.1 and 3.2 million adults use vapes in England alone. Whilst most vapes on the market conform with the required rules and legislation, there are many that do not. These are primarily disposable vapes.

When purchasing a disposable vape, please bear in mind the following:

 It is illegal to sell any nicotineinhaling device with a tank capacity of over two millilitres. It is difficult to provide ironclad advice in this regard, but it is widely accepted



that around 600 'puffs' is acceptable.

 It is illegal to sell any nicotineinhaling device or refill containing over 20 milligrams of nicotine per millilitre (2%). This will generally be indicated on the packaging or device itself in percentages, i.e., 0%, 2% etc.

Between January 1st and February 31st 2023, RCBC Trading Standards have seized 422 non-compliant nicotine-inhaling devices from retailers across the borough. However, we rely on information provided by the public – so if you are aware of the sale of potentially illicit vapes, then please let us know. You can anonymously report such criminality through 'crimestoppersuk.org', who will then pass any information that you provide to us so that we can take action to remove these illicit and potentially dangerous products from the market.

# BOTOX AND COSMETIC FILLERS



Trading Standards has responsibility for enforcing legislation which restricts access to botulinum toxins, (commonly known as Botox), and cosmetic fillers by persons under the age of 18.

In March 2023 Redcar & Cleveland Trading Standards wrote to all the traders in the borough known to administer Botox and fillers to consumers, setting out the requirements of the law in relation to agerestricted sales and provided advice on how to comply.

Further checks will be made to ensure businesses are following the rules.

The law prohibits persons and business owners from administering Botox and fillers to persons under the age of 18. It is also an offence to arrange to administer, or arrange for another person to administer, Botox and cosmetic fillers to persons under 18.

There are many potential health risks associated with these procedures and the purpose of the legislation is to safeguard the health of young people.

### **VOLUNTEER FOR US**

We are looking for volunteers to assist us with underage sales test purchases.

Many products including tobacco, alcohol, knives, solvents, and nicotine inhaling products, are subject to age restrictions.

As part of the approach in enforcing underage sales those who sell from retail premises are tested by using volunteers aged between 12 and 15½ years.

The volunteer would simply attempt to buy age-restricted products while being observed by an officer from Trading Standards.

If you have a child who may be interested please email tradingstandards@redcar-cleveland.gov.uk or telephone 01287 612489.

By taking part in test purchase exercises volunteers help safeguard the health and well-being of local communities and peers and gain an excellent addition to their CV.

Volunteers will be provided with a gift voucher and a participation certificate in recognition of their assistance with this important area of work.



# SAFER COMMUNITIES - Victim Care and Advice Service

The Victim Care and Advice Service (VCAS) provides free, independent and confidential support to victims of crime and anti-social behaviour and their families, throughout the Cleveland area.

We help people to cope with the immediate impact of the crime and assist in their recovery. The service is managed by Safer Communities, a local registered charity with over 25 years' experience. VCAS delivers victim services on behalf of the Office of the Police and Crime Commissioner for Cleveland. We work in partnership to address crime and promote community safety.

For many people the need for support is in the immediate aftermath of the crime being committed but for some the full impact is not evident until later. The service therefore responds to personal circumstances and individual needs at any point following the crime and regardless of whether it was reported to the police or not.

Equally, the impact of crime can have an emotional and physical impact on family, friends and witnesses. They too are welcome to contact the Victim Care and Advice Service for advice or additional assistance.

If you would like further information on our service, please contact Victim Care and Advice Service on 0303 040 1099/01642 664442 or email info@vcas.uk

Facebook- Safer Communities.

Website www.safercommunities.org.uk



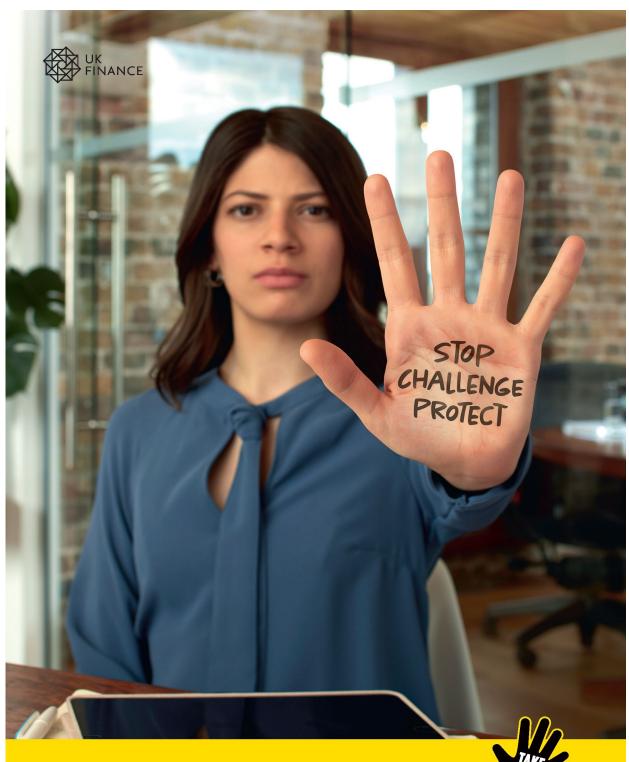
### POP AONG FOR A CHAT

Safer Communities' information events are held at Morrison's Redcar, first Thursday of the month, 1- 2.30pm in and outside of the Community Room









Criminals are experts at impersonating people, organisations and the police. They spend hours researching you for their scams, hoping you'll let your guard down for just a moment.

Stop and think. It could protect you and your money.

TO STOP FRAUD

takefive-stopfraud.org.uk