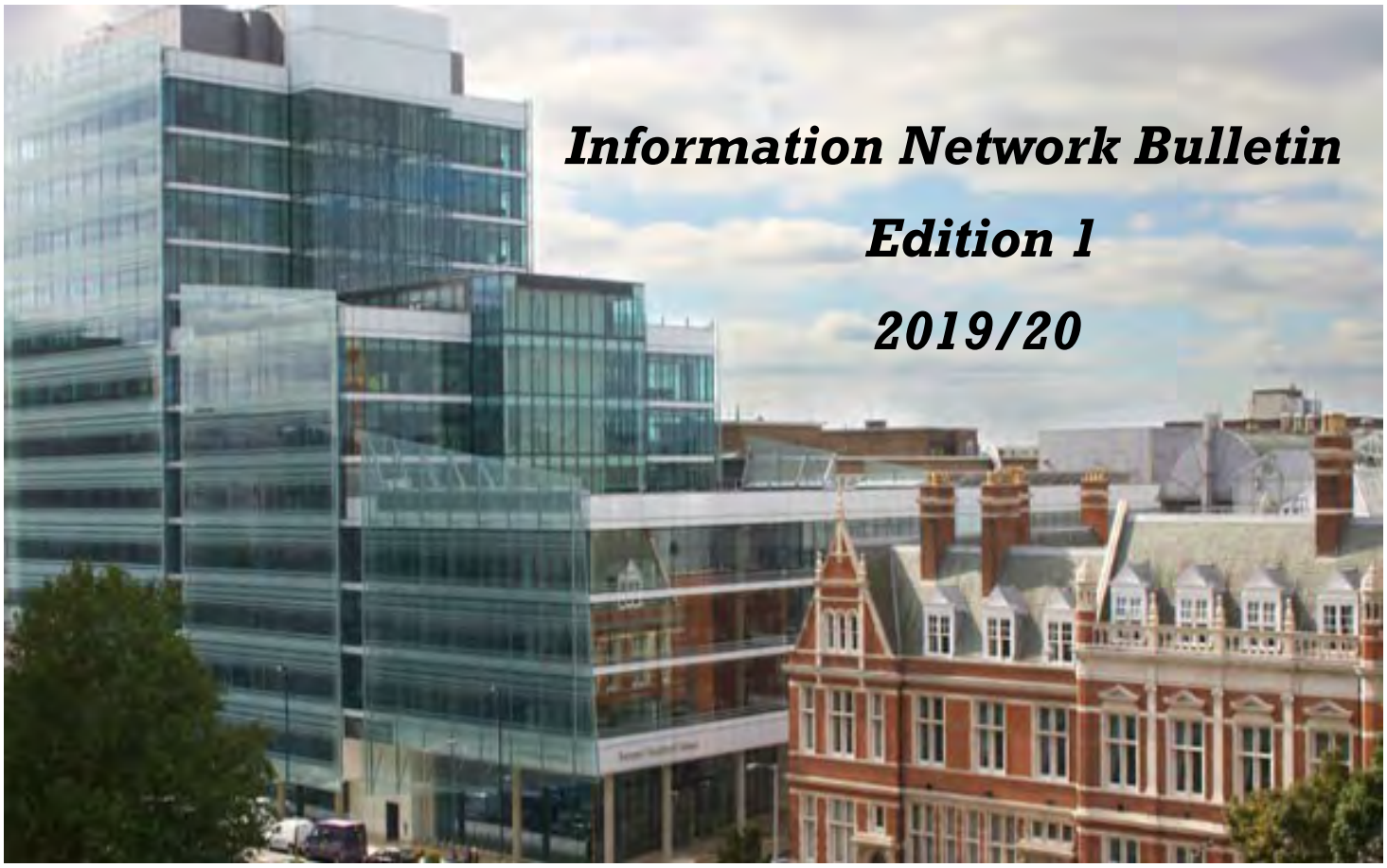


Information Network Bulletin

Edition 1

2019/20

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.

Unhappy with your Landlord or Agent? Don't keep it to yourself

Huge numbers of persons rent property in London. Unfortunately the high demand and rents attract unscrupulous landlords and agents into the market, with bad practices and poor housing.

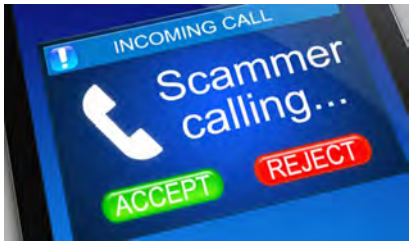
Various organisations work towards stamping out bad practices, but the Mayor of London has launched a website where you can report the bad experiences that you have had with your landlord and/or agent. There are also pages with advice on renting in London, information on rent levels and you can also check whether your landlord or agent has been caught breaking the rules in London before.

As the function is operated by the Mayor of London, you can only make reports referring to properties in London, but it's a good way of raising the alarm about a specific landlord or agent:

www.london.gov.uk/what-we-do/housing-and-land/renting/report-rogue-landlord-or-agent

And if you are happy with your landlord and agent? Then have a look at the other pages and you may find some helpful advice to use when you next move.

Cold Calling Scams



Cold calling scams over the phone involve people making unsolicited calls and deceiving people into believing they are talking to someone legitimate.

There are a huge range of scams but here are some of the more common ones which cause people to lose large sums of money.

- **HMRC Scam**

Automated message stating you owe HMRC money, are liable to arrest, or subject to a lawsuit, which then asks you to Press 1 to make a payment or speak to the officer dealing with your case. **HANG UP**.

If HMRC have an issue, they will write to you and you will be able to call them directly to see what the issue is.

- **British Gas/Energy supplier scams.**

Cold callers will claim you need to pay an outstanding bill or confirm your bank details for a Direct Debit. There are many different reasons used by fraudsters to obtain your bank details. **HANG UP.**

Call your supplier on a number you already have on previous paperwork or emails, to confirm whether the cold call is genuine. **Never give out your bank details over the phone to someone who has called you.**

- **Police/Bank Scam**

The cold caller will state they are a member of the police or your bank and inform you that someone has been caught trying to use your bank details or your card. **HANG UP**.

They will ask you to either attend a bank and give someone money or give your card to a courier who will attend your home or ask you for your PIN – this will be under a ruse to 'catch' someone in the act but the reality is they are just obtaining your bank details and personal information. Your bank should never ask for your PIN number and the police would never ask you to part with your card, money or personal/password/PIN information to assist them like this.

Beware Hanging on the Line

In some cases, they will tell you to hang up and call your bank or the police. However, they leave the phone line open and play a dial tone so when you think you are calling your bank or police they are actually still on the phone and will pretend to be whomever you are calling.

HANG UP. WAIT TWO MINUTES.

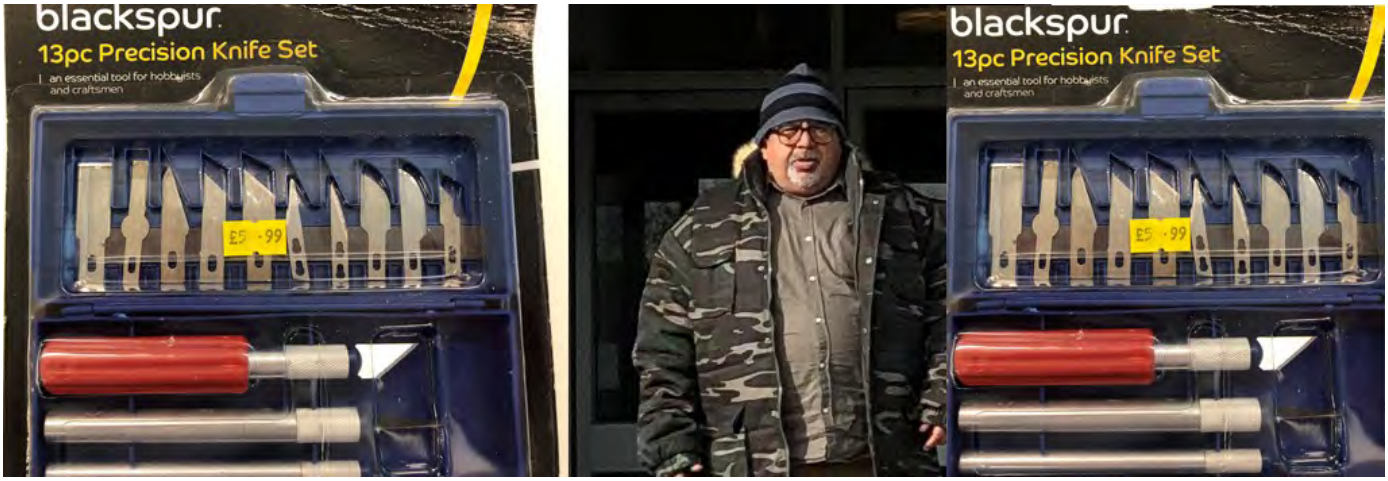
Leave it over two minutes before you pick up the phone and make contact with your supplier, bank, or the police because they can leave the line open for up to two minutes without you realising.

Assistance

If you are receiving unwanted calls you can register your number free of charge to the Telephone Preference Service.

Visit www.tpsonline.org.uk/tps or call 0345 070 0707 to register, get more information on the service, or to report unsolicited direct marketing calls.

Director fined over illegal sale of knives



A company has been ordered to pay over £5,500 after a store employee illegally sold a pack of 13 knives to a schoolchild.

Croydon Council prosecuted Astoria International Limited after a trading standards officer saw an employee at the company's Gift Bank shop in New Addington sell the craft knives on 15 September 2018 to the 14-year-old girl.

On Thursday 21 March, store employee Raymond Morris, who sold the knives, was given a four-month prison sentence suspended for 12 months, ordered to pay £315 in costs and victim surcharge, do 100 hours' unpaid community work and carry out 19 sessions with Think First, a Home Office-accredited rehabilitation programme for offenders. Mr Morris, 56, of Horsley Drive in New Addington, admitted at an earlier hearing the offence of selling a knife product to someone under 18.

At Croydon Magistrates' Court on Tuesday 26 March, Astoria International company director Ram Kumar Vijay, 53, of Norwood Road in Southall, who also admitted the same offence at an earlier hearing, was fined £1,000 and ordered to pay £4,210.80 in costs plus £300 in victim surcharge.

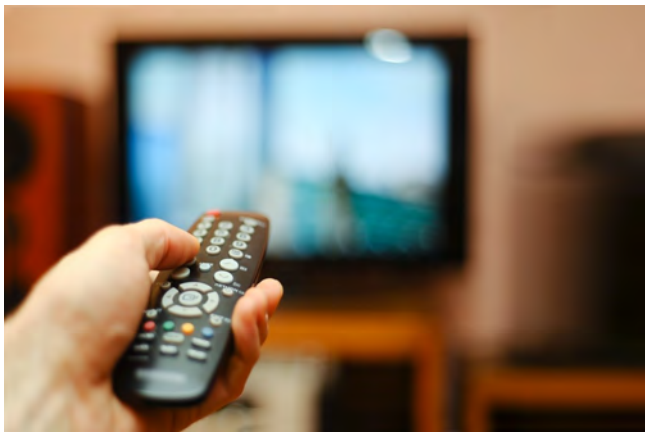
The court heard at a previous hearing that the teenager was a volunteer carrying out underage test purchases as part of regular Trading Standards checks to ensure businesses are obeying the law on knife sales. Under the Criminal Justice Act 1988 as amended by the Offensive Weapons Act 1996, it is illegal to sell a knife, knife blade, razor blade or axe to anyone under 18.

The council's trading standards and Metropolitan Police officers worked together on September's test purchase after police had given Gift Bank a previous verbal warning in April 2018 for selling a two-piece cutter set to two 13-year-olds in school uniform at the store in Central Parade.

Croydon's trading standards team runs regular free training sessions called Do You Pass that keep businesses up-to-date on the law, best practice and to prevent underage sales of age-restricted products. At a previous hearing the court was told that, despite council offers to take up this training and reminders that test purchases would be carried out, the company did not get in touch for the training.

The TV Licensing scam that has cost victims over £830,000 and how to spot it

An ongoing TV Licensing phishing campaign, first identified by the National Fraud Intelligence Bureau (NFIB) in September 2018, continues to be reported to Action Fraud in high numbers.



Fraudsters are sending members of the public fake TV Licensing emails that are designed to steal their personal and financial information.

Since April 2018, Action Fraud has received over 900 crime reports with victim losses totalling more than £830,000.

How you can protect yourself:

• Don't click on the links or attachments in suspicious emails and never respond to messages that ask for your personal or financial details.

• Don't assume a phone call or email is authentic, even if someone knows your basis details (such as your name or address). Remember, criminals can spoof phone numbers and email addresses to appear as companies you know and trust, such as TV Licensing.

• Your bank will never call and ask you for your PIN, full banking password, or ask you to transfer money out of your account.

What to do if you've fallen victim:

• Let your bank know as soon as possible and monitor your bank statements regularly for any unusual activity.

• If you suspect your identity may have been stolen you can check your credit file quickly and easily online. Use a reputable service provider and follow up on any unexpected or suspicious results.

• If you have been a victim of fraud or cyber crime, report it to Action Fraud at actionfraud.police.uk or by calling 0300 123 2040.

Although fraud and cybercrime comes in many forms, there are some simple steps you can take to protect yourself

ActionFraud
National Fraud & Cyber Crime Reporting Centre
0300 123 2040

1. Do not give any personal information (name, address, bank details, email or phone number) to organisations or people before verifying their credentials.

- Always question unsolicited calls, texts or emails requesting your personal or financial information (name, address, bank details, email or phone number). Instead, contact the company directly using a known email or phone number.

2. Make sure your computer has up-to-date anti-virus software and a firewall installed. Ensure your browser is set to the highest level of security and monitoring to prevent malware issues and computer crimes.

- Always install the latest software and app updates on all of your devices. Protect your email account with a strong, separate password and enable two-factor authentication (2FA) where possible.
- Installing, or enabling, antivirus software on your laptops and computers will protect them from viruses and hackers.

3. Many frauds start with a phishing email. Remember that banks and financial institutions will not send you an email asking you to click on a link and confirm your bank details. Do not trust such emails, even if they look genuine. You can always call your bank using the phone number on a genuine piece of correspondence, website (typed directly into the address bar) or the phone book to check if you're not sure.

- Never automatically click on a link in an unexpected email or text.
- Remember, email addresses and phone numbers can be spoofed, so don't use those as a means to verify that a message or call is authentic.
- The best way to get in touch with a company is to use a known email or phone number, such as the one on the back of your bank card.

4. Sign-up to Verified by Visa or MasterCard Secure Code whenever you are given the option while shopping online. This involves you registering a password with your card company and adds an additional layer of security to online transactions with signed-up retailers.

- Layer up your protection. When shopping online, always check the web address to make sure you are on the correct site and sign-up to Verified by Visa or MasterCard Secure Code whenever you are given the option.

5. You should regularly get a copy of your credit file and check it for entries you don't recognise. Callcredit, Equifax and Experian can all provide your credit file. An identity protection service such as ProtectMyID monitors your Experian credit report and alerts you by email or SMS to potential fraudulent activity. If it's fraud, a dedicated caseworker will help you resolve everything.

You should regularly get a copy of your credit file. Callcredit, Equifax, Experian, ClearScore and Noddle can all provide you with a copy. If you spot anything suspicious, make sure your report it as soon as possible.

- If you have been affected by a data breach that leaked your personal or financial details, monitor your credit file and bank accounts regularly for any unusual activity.

(continued next page)

Although fraud and cybercrime comes in many forms, there are some simple steps you can take to protect yourself (cont.)

ActionFraud
National Fraud & Cyber Crime Reporting Centre
0300 123 2040

- An identity protection service such as ProtectMyID monitors your Experian credit report and alerts you by email or SMS to potential fraudulent activity. If its fraud, a dedicated caseworker will help you resolve everything.

6. Destroy and preferably shred receipts with your card details on and post with your name and address on. Identity fraudsters don't need much information in order to be able to clone your identity.

7. If you receive bills, invoices or receipts for things that you haven't bought, or financial institutions you don't normally deal with or contact you about outstanding debts, take action. Your identity may have been stolen.

- Stay in control, destroy your receipts and posts with you name on. If you receive a bill, invoice, or receipts for things you haven't brought or normally deal with, take action. Your identity may have been stolen.

8. Be extremely wary of post, phone calls or emails offering you business deals out of the blue. If an offer seems too good to be true, it probably is. Always question it.

- Listen to your instincts and be wary of unsolicited calls, emails or online ads offering deals that sound too good to be true.
- Genuine banks, or other trusted organisations, won't pressure you into making a financial transaction, if something feels wrong then it's usually right to question it.

9. If you have been a victim of fraud, be aware of fraud recovery fraud. This is when fraudsters pretend to be a lawyer or a law enforcement officer and tell you they can help you recover the money you've already lost.

10. If you need advice about fraud or cyber crime get in with Action Fraud by calling 0300 123 2040.

Home Safety – Appliances and Good Practice

Keep everyone you love and everything important to you safe.

Don't leave appliances such as dishwashers, tumble dryers ad washing machines on when you are out or when you are asleep.

Register your white goods so you will know if a safety issue is identified. There is also information on how to keep your household safe. Visit www.registermyappliance.org.uk

Check for product recalls – visit www.electricalsafetyfirst.org.uk/product-recalls/

Get your free home fire safety visit from The London Fire Brigade.

The London Fire Brigade visited 80,559 homes in 2018 with the aim of helping our communities understand and reduce the risks of fire at home.

By taking some simple precautions you can prevent a fire from happening – making everyone in your home a lot safer. During a visit, our officers will visit you at home, and provide fire safety advice suited to your individuals needs and home.

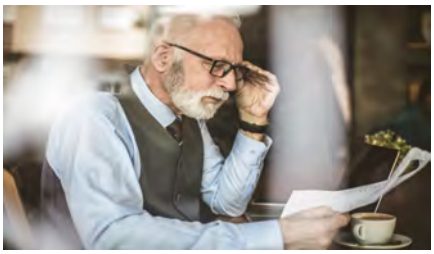
They can also fit free smoke alarms, and specialist alarms for people with visual or hearing impairments.
To book a home fire safety visit please visit:

https://www.london-fire.gov.uk/safety/the-home/book-a-home-fire-safety-visit/

You can also :

- **call free on 0800 028 4428**
- **email smokealarms@london-fire.gov.uk**
- **text/SMS 07860 021 319**

A third of over 75s targeted by investment scams, as FCA urges consumers to take the time to check



The Financial Conduct Authority (FCA) is urging over 55s to take their time to check that Investment 'opportunities' are legitimate before they hand over their money.

- A fifth (22%) of over 55s and a third (32%) of over 75s believe they have been targeted by an investment scam in the last 3 years
- Over half (55%) of those who have invested in financial products did so on their own, rather than making the decision with family
- One in eight (14%) of over 55s spend little or no time researching financial investment products before handing over money, rising to a quarter (26%) of over 75s
- On average, victims of investment fraud lost £32,000 each last year.

To avoid being a victim of investment fraud, the FCA advises consumers to, at the very least:

- Reject unsolicited contact about investments.
- Before investing, check the FCA Register to see if the firm or individual you are dealing with is authorised and check the FCA Warning List of firms to avoid.
- Consider getting impartial advice before investing.

FCA FINANCIAL CONDUCT AUTHORITY

New search tool helps consumers avoid Loan Sharks

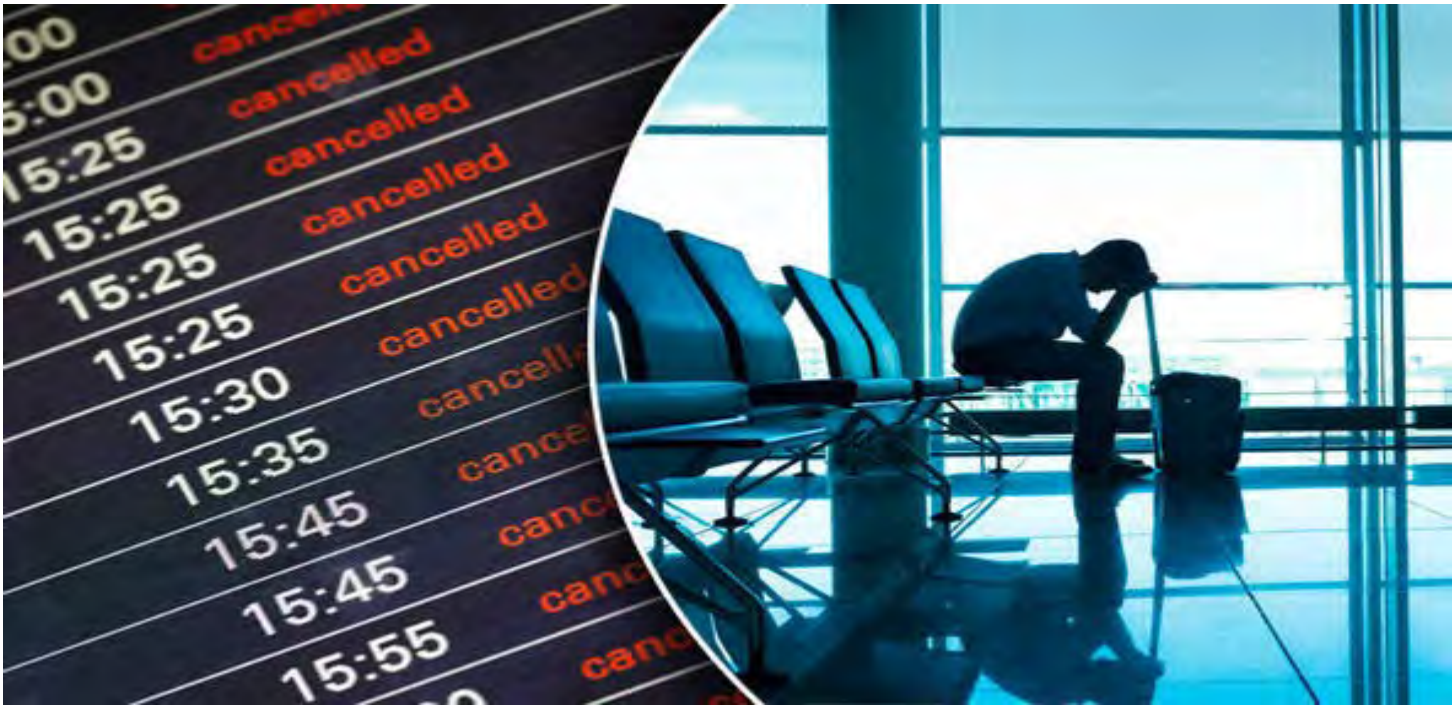
Loan Smart is a new charity formed to help tackle the scourge of illegal money lending. They have recently launched a new website, enabling consumers to check whether their lender is fully authorised by the FCA.

The Loan Smart website draws upon the FCA's registration data to identify fully authorised consumer credit firms. This will help consumers avoid falling into the clutches of illegal loan sharks, complementing the important work already being undertaken by the Illegal Money Lending Teams.

The site also offers consumers practical advice on what to do next if they suspect someone is lending money illegally or where they can get proper help and advice.

Think Loan Smart, not Loan Shark.

Cancelled/Delayed Flight? Got a company keen to help you make a claim? Look out for the bottom line!



These days consumers are entitled to claim compensation for all sorts of things. PPI, being miss-sold chargeable bank accounts and for several years many air-line delays and cancellations.

Passengers whose flights are cancelled, delayed or denied can claim compensation from their airline under EC Regulation 261/2004. Under the rule passengers are entitled to up to €600 if their flight is delayed by more than three hours, unless the delay was caused by an 'extraordinary circumstance' outside of the control of the airline.

There are processes for consumers to follow in order to claim for their compensation. They should contact their airline who will inform them of the course to take, these processes are fairly straightforward, can be done by the consumer themselves and are free.

However, as a result, a multitude of claims management companies have sprung up to take advantage of the compensation that passengers can claim, by acting for them and then charging large fees for the privilege.

Many of these firms advertise online, with their fees in the small print. Some cold call persons at home; while other have been reported as handing out clams forms at airports to holiday passengers arriving on delayed flights.

These businesses promote how helpful they can be in saving passengers the time and worry of dealing with these claims by taking the case on for them. However, the information that passengers must give them to process the claim is the same as that required if the passenger claimed direct from their airline, so they could do it just as easily themselves. What these businesses don't promote is the large fees that they charge for allowing them pass your claim information to the airlines for you.

So if your flights to or from some winter sunshine are cancelled or delayed:

- contact your airline directly
- complete the claims forms yourself

Remember the bottom line!

Renters urged to spot the signs of Tenancy Deposit Scheme fraud

Action Fraud has received reports of fraudsters claiming to be landlords of rented properties available online.

- Action Fraud is warning the public that fraudsters are claiming to be landlords to trick people into paying upfront 'rent' into Tenancy Deposit Scheme (TDS).
- This comes as 28 reports were made to Action Fraud between December 2018 and February 2019 alone – amounting to a total loss of £19,990.

How is this happening?

Action Fraud has received reports of fraudsters claiming to be landlords of rented properties available online. Prior to viewing the property, the fraudster asks the victim to pay a deposit and in some cases a month's rent upfront. They claim that the money will be protected by Tenancy Deposit Scheme and that the money is safeguarded under Government legislation.

After the individual pays the money, the fraudster sends a bogus email claiming to be from Tenancy Deposit Scheme confirming they have received their deposit. Victims are later discovering that the money is being sent directly to the fraudster and that they have been left out of pocket and with no home to move into as a result.

What you should do:

- Always make sure you, or a reliable contact, has viewed the property with an agent or landlord before agreeing to rent a property.
- Don't be rushed or pressured into making a decision. Only transfer funds when you're satisfied a genuine property, safety certificates and valid contract are in place.
- Only pay for goods or service by bank transfer if you know and trust the person. Payments via bank transfer offer you no protection if you become a victim of fraud.
- Once you've paid your deposit, you can check whether it's protected by entering your tenancy deposit certificate code on TDS website.
- **Every report matters** – if you've been a victim of fraud or cyber crime, report it to Action Fraud online or by calling 0300 123 2040.

UK ECC offer advice to customers of Wow Air following shutdown

UK holidaymakers affected by the collapse of Wow Air should contact the UK European Consumer Centre (UK ECC) for help and advice, following the announcement that the airline will cease operations immediately

The airline, which is based in Reykjavik, Iceland, stopped operating on Thursday 28 March 2019, with some passengers stranded and others no longer able to take up their booked flights. Wow Air have ceased communication and requested customers make alternative arrangements with other carriers.

The UK ECC can provide advice and support to consumers affected by the collapse. Consumer Advisor at the UK ECC, Adam Mortimer, said: “Passengers who have already travelled will need to make their own arrangements to return home. Some airlines, such as Icelandair and Easyjet, are offering to assist Wow Air passengers with discounted fares.”

“It is highly probable that passengers will need to contact their insurer to arrange reimbursement of any extra expenses for their return home.”

For more details, check out the UK European Consumer Centre’s website or contact the UK ECC for free advice on your individual circumstances on 01268 886690 Monday-Thursday between 10 am and 4 pm (or email ECCNET-UK@ec.europa.eu)

The UK ECC is part of the European Consumer Centre Network (ECC-Net), which has 30 centres in the EU, plus Iceland and Norway. The aim of the network is to provide advice and support to consumers who have a dispute with a trader based in a European country outside the UK

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: **03454 04 05 06**
Web: **www.citizensadvice.org.uk**