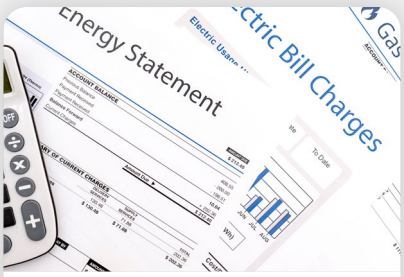
tiaa

FRAUD STOP

Winter 2022

New Look!

ISSUE

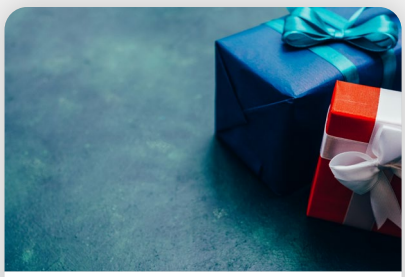


SCAM ALERT
Energy scams during the cost of living crisis

→ SEE PAGE 2

COURT ROUND UP
Cases in court

→ SEE PAGE 3



BRIBERY ACT COMPLIANCE
What all organisations need to consider

→ SEE PAGE 4

Introduction

The Office for National Statistics say that people are more likely to fall victim to fraud and cyber offences above any other crime. Organisations also face a growing risk of fraud.

The National Crime Agency reports that cyber-crime continues to rise in scale and complexity with the activity affecting essential services and businesses alike. In this edition of Fraud Stop we will be providing insight into real cases along with practical advice and guidance to aid in the identification and prevention of cyber related fraud.

In July 2022, Cifas (the UK's Fraud Prevention Community) predicted that fraud cases were set to soar amidst the cost of living crisis as criminals bet on economic uncertainty.

This edition also considers how the rise in the cost of living is providing criminals with new opportunities to steal personal and financial information. The impact of this activity is increased pressure on individuals and businesses. The potential for individuals to rationalise their behavior along with the increased pressure and potential increased opportunity creates the perfect environment for fraudulent activity.

Scam alerts during the cost of living crisis

Action Fraud, the National Fraud and Cyber Crime Reporting Centre, has issued a warning about the following scam currently in circulation:

Criminals are exploiting the cost of living crisis and targeting the public with energy rebate scams.

1500 reports have been made to the National Fraud Intelligence Bureau regarding scam emails about energy rebates purportedly from Ofgem, the independent energy regulator. The scam emails claim that the recipient is due a rebate payment as part of a government scheme and provides links for the recipient to follow to apply for the rebate. The links lead you to malicious websites designed to steal your personal and financial information. The subject header of the emails states "Claim your bill rebate now" and the Ofgem logo and colours are used so that the email appears authentic.

This is an example of authorised push payment scams when criminals trick you into sending money directly from your account to an account controlled by the criminal.

REMEMBER:

- **STOP -** Take a moment to stop and think before parting with your money and giving out information
- **CHALLENGE -** It could be fake, so it is OK to refuse any request. Only criminals will try to rush you
- **PROTECT -** Contact your bank immediately if you think you have been a victim of a scam and report it to Action Fraud
  Reporting fraud and cyber crime

Similar frauds relating to the cost of living crisis include:

- Texts or emails from your energy supplier similarly diverting you to malicious websites.
- Prepayment meter tokens being cloned and sold at a reduced price, but your energy supplier never receives the payment and the tokens are fake.
- Scammers offering better fixed rate deals if you switch urgently – the scammers will be after your bank details.
- Energy saving devices being sold online claiming to cut your monthly bills. They are unlikely to work and are also a safety hazard.

Cases in court

Full details of the following three cases can be found at https://www.cps.gov.uk/news

In July 2022 four fraudsters were imprisoned for a mass investment fraud worth over £13.7 million, and were sentenced to a total of nearly fifteen years in prison or on license. The fraudsters persuaded victims to invest into a fund said to generate income through buying, upgrading and selling residential properties through a company called Essex and London Properties (ELP). The company however did not own the properties, many of which were not even on the market. The investigation uncovered that more than 800 people had invested in this bogus scheme. Victims made payments that ranged from £5,000 to £140,000 to ELP. ELP claimed to have bought properties along the Crossrail route running from London to Essex which would then be refurbished and re-sold at a profit. However only one property was ever bought.

Two scammers were jailed in July 2022 for a pension fraud worth over £20 million which caused many of the victims to lose their entire pensions. Each of the scammers were sentenced to six years imprisonment for conspiracy to defraud and money laundering. The duo devised a plan to persuade pension holders, predominantly Equitable Life customers, to transfer their pensions into accounts controlled by one of them. The customers were persuaded to sign application forms which had blank sections, later completed by the scammers and enabled them to take control of the pension funds. Without the knowledge of the victims, funds were placed into high risk and wholly unsuitable offshore investments. These investments provided the two defendants with high rates of commission but put the pension funds at risk. A number of those pension funds have subsequently collapsed, resulting in some pension holders losing substantial amounts of their pension provision. Some victims lost their whole pension. The duo extracted around 10% of the gross sum in unauthorised commission payments – in excess of £1 million each – for their own benefit.

An IT fraudster was jailed in June 2022 for profiting by more than £1m from selling software which allowed criminals to dupe people into divulging personal banking information. The fraudster pleaded guilty to two counts of supplying computer software for fraudulent purposes and one count of money laundering and was sentenced to four-and-a-half years' imprisonment. The police investigation revealed that the criminal used an online messaging app, Telegram, to offer specialist software for sale which enabled other fraudsters to bypass banking security systems. The software was offered through a monthly subscription, charging a fee of around £600 per month, payable in cryptocurrency. Over a period of around eight months, the criminal made over £1.3 million worth of sales of the product to over 1000 fraudsters. It is unclear how many fraudsters might have used the software or the scale of potential victims and losses.

In other news, the BBC has reported that a University of Brighton staff member has been arrested over allegations of fraud. The university first became concerned something was amiss last year, and hired forensic accountants to investigate. Sussex Police said they had arrested a member of university staff on suspicion of fraud by abuse of position and by misrepresentation, and had released them under investigation.

The BBC also reports that the former head of a private girls' school has appeared in court charged with expenses fraud and theft. They are accused of submitting fraudulent John Lewis expense claims and stealing an iPad Pro from the school. The former head, who has been sacked from their job, has denied fraud and theft and will stand trial in August 2023.

A large scale fraud investigation was undertaken by Merseyside Police into fraudulently signed building cladding safety forms. The defendant pleaded guilty to providing 53 EWS1 forms to property management companies. EWS1 forms were introduced following the Grenfell disaster so that residents could get their building's cladding assessed for potential fire risk. The forms require an appropriate person to confirm the checks have been completed but residents of high-rise buildings reported that forms had been signed off by a person not authorised to sign them. The fraudster was sentenced in September 2022 to a 15 day rehabilitation order and 200 hours unpaid work, plus court costs of £1500. The correct checks have since been completed.

Bribery Act Compliance

It is a requirement under the Bribery Act 2010 that organisations should have adequate procedures in place to prevent bribery, and a robust policy should cover as a minimum declarations/conflicts of interest, gifts and hospitality, record keeping and business conduct standards. It is recommended that the effectiveness of the implementation of the process and staff awareness of the requirements of the policy are regularly tested.

CONSIDER:

- **Proportionality: The action you take should be proportionate to the risks you face and the size of your business.**
- **Top level commitment: Those at the top of an organisation are in the best position to ensure their organisation conducts itself without bribery.**
- **Risk assessment: Think about the bribery risks you might face given the specific context of your organisation, its activities and areas of operation.**
- **Due diligence: Knowing exactly who you are dealing with can help to protect your organisation from taking on people who might be less than trustworthy.**
- **Communication: Communicating your policies and procedures to volunteers, staff and partners will enhance awareness and help to deter bribery.**

Social Media – Dos and Don'ts when reporting fraud

Social media is typically used for social interaction and access to news, information and decision making and has rapidly become part of daily activity. It is a valuable communication tool locally and worldwide, as well as to share, create, and spread information. It is therefore important to bear in mind what you should and should not do when using social media in relation to reporting an allegation of fraud.

Don't:

- DO NOT tag a person or organisation, such as TIAA or an Anti-Crime Specialist in a LinkedIn, Facebook or Twitter post to report an allegation. This does not constitute making a report. These are not the appropriate platforms to report an allegation and are not monitored 24/7
- DO NOT share images of your report or any evidence online on social media
- DO NOT share details of the allegation, including names on social media

Do

- Contact only the named person you have been provided contact details for to discuss your concerns, or email fraud@tiaa.co.uk

TIAA Anti-Crime Specialists have been trained by ACAS to conduct workplace investigations.

If your organisation requires any proactive or reactive counter fraud support or advice, contact;

Melanie Alflatt, Director - Risk and Advisory, Email: fraud@tiaa.co.uk