COVID-19 Fraud & Security Alerts

Ref: CFMG-0016

NHS Counter Fraud Managers Group (CFMG)

Supported by TIAN and 360 ASSURANCE

NHS supplier mandate fraud attempts

This appears to be a recurrent theme recently, we have been alerted that a further two NHS suppliers have warned customers of mandate fraud attempts.

- Edmundson Electrical Ltd has reported a mandate fraud attempt. They have been contacting Finance personal to confirm that their payment details have not changed.
- Oncology Imaging Systems Ltd (OIS) has also identified fraudulent email claims requesting changes to payment details due to the Covid 19 Pandemic. OIS has written to their customers and given advice on precautions to take as follows:
    - Confirm the sender's identity before replying to email requests and before opening attachments or clicking on links, even if they appear to come from a legitimate source.
    - Consult your Information Technology department about any phishing attempts.
    - Call to validate communications originating from OIS. Visit their official website or phone their advertised phone number. Don't use the links or contact details in the message you have been sent.

British Dental Association members targeted by hackers

The British Dental Association (BDA) has suffered a data breach causing fears that the bank account numbers of a number of UK dentists have been stolen. The BBC has reported that the professional association emailed its membership to warn them of the breach, telling them it is currently unsure what information has been accessed. The BDA also urged them to be vigilant about any correspondence purporting to be from a bank. It was reported that while the organisation does not store its members' card details, it does hold their account numbers and sort codes in order to collect direct-debit payments

Read BBC article here

Police charge 'fake psychiatrist' who worked for NHS for 22 years despite having no qualifications' with 13 fraud offences

A fake psychiatrist who worked for the NHS for 22 years despite allegedly not having any qualifications has been charged with 13 fraud

offences, following an investigation by detectives in the area's Crime and Safeguarding Team. The Cumbria Constabulary confirmed the former NHS worker had been charged with two counts of making a false instrument with intent it be accepted as genuine. She has also been charged with eight counts of fraud by false representation and three counts of obtaining a pecuniary advantage. She worked as a locum consultant psychiatrist for the Norfolk and Suffolk Foundation Trust (NSFT) between 2014 and 2015, mainly looking after disabled adults and children.
Read full article here

164 Instagram users report losing over £350,000 to investment scams

During June 2020, Action Fraud received 164 reports from individuals falling victim to fraudulent investment schemes, commonly referred to as a 'money flipping' service offered by users on the Instagram social media platform. These reports have amounted to a combined financial loss of £358,809. The individual financial losses from this fraud smaller and targets a younger demographic, typically aged between 20 and 30, with less savings or those who are financially vulnerable and are searching for a quick and easy way to make money.

The scheme involves fraudsters approaching victims via the instant messaging feature of the platform after advertising their service. They claim to only require an initial investment of a few hundred pounds which they say will be invested and multiplied several times within a matter of days and then paid back to the victim after a small commission is deducted for the service. However, once the initial investment received additional funds are requested until eventually all contact is severed and the victim is blocked by the suspect. Victims are usually requested to send the money by bank transfer or through a cryptocurrency platform which means it is nearly impossible to retrieve.

Read full article here

Audit Wales: public sector fraud needs to be taken seriously

Audit Wales has issued a report on public sector fraud in Wales and stated that fraud in the Welsh public sector could be costing up to £1bn a year. The report also identifies seven key themes that public bodies need to focus on and counter-fraud arrangements need to be strengthened, particularly in local government. The seven key themes are: leadership and culture; risk management and control frameworks; policies and training; capacity and expertise; tools and data; collaboration; and reporting and scrutiny.

Similar topics and recommendations were contained in a report commissioned by the Ministry of Housing, Communities & Local Government (MHCLG) into fraud in local government procurement.

Read the ICAEW insight here

Covid 19 and Fraud Risk: Managing and responding in times of crisis

Companies across various industries are experiencing increased operational and financial pressure due to the COVID-19 pandemic. These pressures create a heightened level of economic risks which may lead to increased motivation or justification to commit fraud, through manipulation of financial results, misrepresentation of facts, misappropriation of assets and other fraud schemes.

Deloitte publication

Over £44,000 lost to a PayPal scam that uses hacked Facebook accounts to lure victims

A new alert from Action Fraud and the National Fraud Intelligence Bureau regarding PayPal scams showed that 95 people have reported losing over £44,000 to a PayPal scam that lures in victims using hacked Facebook accounts.

Read Action Fraud article here

HMRC investigate over 10,000 COVID related scams

Info Security Magazine has reported this week that over 10,000 communications purporting to be from HMRC are being investigated. The communications include emails, SMS, social media messaging and phone calls. Figures provided following a Freedom of Information (FOI) request show that the highest number of reported scams occurred in May 2020, with 5152 reports. This represents a 337% increase compared to March when the UK introduced lockdown restrictions. The article also highlights that HMRC requested the removal of 292 scam websites, as fraudsters used Coronavirus related topics in an attempt to trick victims.

Read the article here.

Serious Fraud Office to expect an increase in pandemic fraud

The Telegraph has reported that experts have warned that the Serious Fraud Office (SFO) is likely to see an onslaught of pandemic related fraud. Sam Tate, a partner at a law firm specialising in white collar crime, believes that the next six to twelve months will likely bring a significant increase in the number of serious fraud cases uncovered, The article notes the director of the Serious Fraud Office, Lisa Osofsky, has recently said that her two years at the agency have been focused more with closing existing cases then pursing new ones. The Telegraph notes that the pandemic may offer the SFO the opportunity to launch more cases and improve its mixed performance of recent investigations.

Read the article here.

Lockdown causes 66% jump in scams

This week The Independent has reported that fraudsters have used the coronavirus pandemic to exploit the public with scams. Research by banking group Barclays shows that frauds increased by 66% in the first six months of 2020. The article continues that the data suggests the trend shows no sign of decreasing, with July showing a 5% increase compared to the previous month. However, it is thought the spike in July may be as a result of investment scam reporting, as victims may not initially realise they have been victim to a scam. Barclays note that there has been a particular increase in online marketplace sites, for example targeting the summer holiday market with false adverts of campervan sales. Another theme identified by Barclays was the significant increase in cryptocurrency related scams

Read the article here.

BBC report on Coronavirus romance scams

As a result of the isolation caused by the Coronavirus lockdown fraudsters have taken advantage of this to target the vulnerable with romance scams. This week the BBC has reported on the issue, detailing the increase in the type of scam during lockdown with accounts from victims. The

article follows the story of Beth who fell victim to a scammer. Typically romance scams involve building the trust of a victim, which lead to requests for financial support.
Read the BBC article here.

Fraud Advisory Panel

The Fraud Advisory Panel latest updated on 20 August 2020 includes; 'current COVID19 fraud risks', most of which we have covered in our weekly alerts; 'Anticipated and/or emerging issues'; and 'some simple preventative tips', with links to some useful documents and contacts.
Read more here

Friends Against Scams virtual session

Friends Against Scams in association with National Trading Standards are delivering a more in-depth session on scam awareness following the success of the July 2020 virtual scam training session. The new session is a more in depth course and is aimed at those who would like to deliver the "Friends against Scams" training to others. It will give you the tools and resources to enable you to deliver the training to your friends and family, communities, organisations and/or as a volunteer for Trading Standards. The session will take place on the 26th August from 10:30am – 12:30pm, via Microsoft Teams. To book on the session email natalie1.webb@surreycc.gov.uk
Click here for more information.

Other type of fraud examples

Email scams & Phishing scams

- TV Licensing continues to be targeted by Fraudsters. Fraudsters are targeting pensioners, pretending to be TV licensing officers and falsely claiming that individuals need to set up new direct debit agreements. Read more here

Social Media

- An ASDA Facebook phishing scam is doing the rounds - Fraudsters are currently targeting Facebook users offering £1,000 gift card offers to women specifically 'born in October'. Around 100 users have already reported seeing the advert on Facebook, which claims that the supermarket is giving away the gift cards to raise brand awareness and asks users to complete a short survey. This survey is designed to steal personal details which can be used for identity fraud. Read article here

Phone

- Cifas has warned that phone scams going viral, with 9 sick cons designed to steal your money and logins. Smartphone scams are on the rise and many iPhone users are finding themselves the targets. A range of scams including fake account warnings, contact tracing scams,

Covid-19 testing scams, free face masks, fake pandemic emergencies, tax and refund scams, fake charity calls & small business scams.

- Action Fraud are aware of a new scam circulating where criminals are contacting victims claiming to be from Action Fraud. If such a call is received claiming to be from Action Fraud or an automated message asking if you wish to speak with an adviser, hang up immediately. Action Fraud can be contacted directly by calling 0300 123 2040 to confirm whether the call was genuine. Action Fraud will never call and ask for your bank account details or to verify your PIN number. If you have handed over these details, call your bank immediately.
- Diners at the Ritz hotel in London have been targeted by scammers posing as hotel staff to steal payment card details. These fraudsters have been phoning customers with exact details of their restaurant bookings and asking them to confirm their payment card details which are then used to purchase goods online. The Ritz has said it has been made aware of a potential data breach is continuing to investigate how the scammers accessed customer information. The Ritz has emailed all customers that may have been affected to confirm that their staff will never contact them by telephone to request credit card details or to confirm their booking. Read BBC article here

Other

- Greater Manchester Police (GMP) are warning of a timeshare fraud. Timeshare fraud involves an investment scam that claims you can easily become a property millionaire from buying a timeshare. You are asked to attend a timeshare presentation and might be pressured into signing a contract for the timeshares which might not exist or fall well below standards described. Click here for more information from Action Fraud
- Another fraud being reported by GMP is rental fraud, which is when would be tenants are tricked into paying an upfront fee to rent a property. Click here for more information from Action Fraud