COVID-19 Fraud & Security Alerts

February 2021

NHS Counter Fraud Managers Group (CFMG)

Supported by TIAN and 360 ASSURANCE

Fraud alert: Scam text regarding COVID vaccines

360 Assurance have been made aware of patients receiving unsolicited text messages containing incorrect information regarding COVID vaccines. In this instance, the text messages states that the vaccination a patient has received is from a 'suspect batch' and to contact a given mobile number as soon as possible. If staff or patients receive such texts they should report their concerns to Action Fraud via 0300 123 2040 or via https://www.actionfraud.police.uk/.

Norfolk and Suffolk NHS Foundation Trust boss faces review over law degree

The BBC has reported that the incoming chief executive of an NHS Trust in special measures faces an inquiry into his qualifications. Annual reports to parliament state Mason Fitzgerald holds a Master of Laws (LLM) from the University of Georgia in the United States, though the university said he did not graduate. Norfolk and Suffolk NHS Foundation Trust said a review had begun.

Read the full BBC article here

Police warn elderly over fake NHS COVID vaccine scams after one victim lost £30,000

Elderly victims of COVID-19 vaccine scams have been warned about the dangers of losing their life savings. Fraudsters are sending out fake NHS texts and emails to exploit the public's eagerness for an appointment to receive the jab. In one example, the Metropolitan Police said smishing messages were texted to patients telling them they are eligible for the vaccine. After clicking on the link, victims are directed to a website with bonus NHS branding that demands bank account details to verify a billing address. The oldest victim so far is 80 years-old and targeted for £30,000.

Read the full article here

Fraudsters pose as fake NHS workers to access homes

Doncaster Superintendent Neil Thomas has said there has been an increase in criminals targeting vulnerable people in the form of NHS staff 'testing for COVID-19 in the home', and to assess their eligibility for a vaccination. Read the full article here

COVID fraudsters caught selling fake coronavirus vaccination cards on eBay

Fraudsters have been caught selling fake coronavirus vaccination cards for £1.49 on eBay, and falsely claiming the money collected is for NHS charities. The Sun was able to buy one from a firm who said that 10% of the money went to NHS Charities Together. The charity, which has spearheaded a £140 million fundraising drive during the pandemic, have said they were horrified by the claims and would be investigating.
Read the full article here

Warning as criminals sell fake COVID-19 vaccines

The European Anti-Fraud Office (OLAF) has issued a warning about fake COVID-19 vaccines. OLAF has heard of reports of fraudsters selling fake vaccines in the EU, as well as fake COVID-19 protection products. Since opening its investigation in March, OLAF has helped identify more than 1,000 suspicious operations and have seized more than 14 million items, including faulty face masks and fake test kits.
Read the full story here

NHS vaccine scam warning: Britons targeted by fake email

The NHS has issued a COVID-19 alert, warning Britons to be vigilant after it emerged many had been targeted by a new and dangerous email scam relating to the vaccine. Many Britons reported receiving emails which invites them to enter their bank details into a website in order to confirm their vaccination appointment. Emails of this kind are simply scams which are designed to part unsuspecting victims with their personal information.
Read the full article here

Three men arrested amid inquiry into £6million COVID-19 loan fund

The Guardian have reported that three men haven been arrested as part of an investigation into fraudulent coronavirus bounce-back loans totalling £6million. Then National Crime Agency (NCA) said all three men worked for the same London financial institution and are suspected of using their 'specialist' knowledge to carry out the scam. The £6million in bogus claims is believed to have been made through the use of false data and documents.
Read the full article here

Woman jailed for trying to con NHS out of £5.7million as she jetted off around the world

Linda Metcalf claimed she could hardly walk or stand, rarely went out and couldn't even dress herself. Ms Metcalf claimed that because of her local trust's negligence she needed walking sticks and was unable to drive. But when put under surveillance it was discovered that instead of being housebound, she had been travelling to the other side of the world. Between her visits to the doctors to pursue her claims, she had visited New Zealand, Fiji, Hong Kong, Lanzarote, Tenerife, Thailand, Wales, Scotland and Scarborough. Ms Metcalf launched her claim for medical negligence against her local NHS Trust after a 24 hour delay in a diagnosis of a spine condition. She claimed as a result she needed an adapted home big enough for a carer, compensation for loss of earnings and childcare funds. After admitting lying about the extent of her mobility problems, Ms Metcalf was sentenced to 6 months imprisonment. Read the full article here

Woman who faked having cancer to defraud well-wishers is jailed

A woman from Kent has been jailed for 2 years and 9 months after scamming well-wishers out of over £45,000 by fraudulently claiming she had cancer. Nicole Elkabbas, claimed that she needed the money for hospital treatment, after being diagnosed with a rare form of ovarian cancer which required her to travel to Spain for surgery, but instead used it to fund an online gambling addiction. Detectives also discovered that the doctors she had claimed to have treated her for cancer either didn't exist or had no record of her on their books.

Read the full article here

Barclays records sharp increase in scams during 2020 as fraudsters capitalised on public uncertainty

Barclays have reported that more people than ever were targeted by scams in 2020. During the months of July to December, the value of fraudulent activity jumped by 66% as scammers capitalised on public uncertainty during the coronavirus pandemic, Barclays have said. This vast increase was driven by high-value and complex scams, with the steepest claims coming from investment scams and impersonation scams.

Read the full article here

Anti-fraud Santander bank worker jailed for customer con

A member of Santander's anti-fraud team has been jailed for selling customers' details in a £90,000 scam. Bilal Abbas, helped conmen buy luxury goods using stolen account details. The transactions would be flagged as fraudulent and cancelled several days later leaving businesses out of pocket. Abbas and two others were jailed for at least 2 years and Newcastle Crown Court.

Read the full BBC article here

Scam alert: fake Barclays 'unusual payee request' text

Which? has reported a scam text message targeting Barclays customers by directing them to a fake website. This text message manages to successfully drop into people's inboxes with the sender set as the bank itself. These types of smishing attempts work by rushing people into visiting a fake website which can then go onto request and steal sensitive information, such as bank account details.

Read the full Which? article here

Romance fraud on the rise in coronavirus lockdown

According to UK Finance, there was a 20% increase in bank transfer fraud linked to romance scams in 2020 compared to 2019. Around £68million was lost to such scams in 2020, another increase on the previous year, said Action Fraud. In both 2019 and 2020 the amount of money lost to romance fraud outweighed that stolen by online shopping fraud, the COVID-19 pandemic has added to the problem.

Read the full article here

Chester village store manager's £21,000 fraud to fund gambling addiction

A Co-op store manager defrauded the company out of £21,000 to fund his gambling addiction. The area manager was made aware of a series of high-value being made at the store, and after checking CCTV, David Knight was found to be processing fictional refunds through the till without

any customers present. A full investigation revealed Knight had been processing through fake Paysafe vouchers and making the money by recording them as sales. Knight was handed a 14-month suspended prison sentence.
Read the full article here

Fraudster spent £175,000 on Premier League footballer's credit card
Sharif Mohammed treated himself to a stay at the Shangri-La, a £20,000 Ibiza holiday and spent £1,400 on Armani Jeans using a footballer's bank card. In total, Sharif Mohammed got away with spending £175,000 on Man City's Riyad Mahrez's credit card, it took over a month for Mahrez to realise he was being defrauded. Truck drive Mohammed spent some of the money at Aspers Casino in Westfield shopping centre as well as on food such as Nandos, KFC and Greggs.
Read the full article here

A National Insurance number phone call scam
It has been reported that there has been a growing number of reports from people who have received an automated phone call which states that their National Insurance number has been "compromised". The recipients are then instructed to "press one on their handset to be connected to a caller", which will allegedly fix the problem. However, doing so can lead to the fraudsters gaining control of your personal details which could lead to terrible consequences for victims.
Read the full article here

Scam alert: Just Eat 'gift card' phishing email
Which? have published that they have received multiple reports of a fake email purporting to be from takeaway delivery service Just Eat. With so many people using takeaway delivery services during the pandemic it is no surprise to see scammers looking to take advantage of those brands. The fake Just Eat email appears to the receiver to be from a Just Eat email account, but if has been deceptively spoofed from contact@Just-Eat.com. The email offers the chance to 'claim a £50 Just Eat gift card' but Which? state that this will almost certainly take you through to a phishing website that will attempt to steal sensitive information. Just Eat has confirmed that the email is fake.
Read the full Which? article here

Fraudster claiming inability to work caught with three jobs
Adam Reason exaggerated an inability to work in order to scam his insurer out of £2,000 a month through an Income Protection Policy, this type of policy is designed to support individuals in the event they cannot work due to illness or injury. If Reason had been successful in continuing his claims, until the expiration of his policy, he could have incurred a potential loss of £648,000 to Aviva. Reason was sentenced to 18 months imprisonment, suspended for 2 years, 150 hours unpaid work and a five day rehabilitation activity requirement for one count of Fraud by False Representation.
Read the full article here

Unqualified court interpreter sentenced after working on 140 cases

Mirwais Patang stole the identity of a legitimate court interpreter and provided services to the courts in 140 cases, despite actually having no qualifications to do so. Patang was sentenced to 2 years imprisonment, suspended for 2 years, on 12 February 2021. He must also complete 300 hours of unpaid work within 24 months.

Read the full article here

HMRC scam: Britons warned about phone call which threatens arrest

HMRC scam phone calls are circulating in a dangerous scam, where Britons are told they have undertaken tax fraud and could be arrested. Several Britons have reported receiving a phone call which informs them there is supposed tax fraud associated with their name. Individuals are then directed to 'press one' on their phone to speak to an advisor about the situation, if they fail to do so they may face a warrant for their immediate arrest. The correspondence is simply a scam, designed to get people to part with their personal details.

Read the full article here

Scam awareness training

Buckinghamshire and Surrey Trading Standards are pleased to offer 2 scam awareness training sessions this March:

Friends Against Scams – 11th March 2021, 15:00 – 16:30

The "Friends against Scams" course raises awareness of scams and what to look out for and is aimed at anyone who would like to learn more about scams and how to deal with the different ones operating. After the course you will be recognised as a "friend" of the scheme and will be encouraged to talk to your friends and family about it, to help others become more scam aware.

ScamChampion session - 16th March 2021, 14:00 – 16:00

Completed the Friends Against Scams session and wish to spread scam awareness further? Why not sign up to our ScamChampion course, where you'll be given the tools and resources to enable you to deliver the Friends Against Scams training to family and friends, colleagues, communities or even as a volunteer for Trading Standards.

You will need to have carried out the online FAS training prior to attending: http://www.friendsagainstscams.org.uk/elearning/surreybucks or attended one of our live Friends Against Scams sessions, such as the 11th March course. Please email natalie1.webb@surreycc.gov.uk to confirm attendance on each/either course, or if you'd like to find out about alternative dates. Find out more about the scam awareness training here