# COVID-19 FRAUD ALERTS

Welcome to Issue 9 of our Covid-19 Fraud Alert newsletter.

We have summarised recent fraud trends in this newsletter for you to be aware of. Please feel free to contact your Local Counter Fraud Specialist for advice on any type of fraud, our details are on the last page.

## NHS Related Alerts

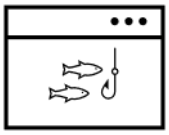
### Potential Covid-19 Vaccine Patient Fraud

As the roll out of the new Covid-19 vaccine approaches, there is the potential that people may impersonate NHS staff in order to gain early access to the programme. NHS lanyards are available for purchase online, and the names of NHS employees may be identifiable through public facing websites (e.g. GP surgery websites often feature a list of employees and their roles to increase engagement) and social media.

As always, please be careful with your social media accounts, being especially mindful of who is able to see what you post, and beware of how much information you can potentially give away which could then be used to impersonate you (e.g. your job role, place of work, length of service etc.)

Please also make sure you are always aware of the whereabouts of your staff ID card. If you think your ID has been lost or stolen, let your security team and/or line manager know immediately.

### Use of Covid-19 Vaccination in Phishing



Europol is predicting that cyber-enabled fraudsters are likely to shift their tactics to exploit the public's interest in the vaccination programme, by sending Covid-19 Vaccination themed phishing emails. It is also likely that they will use other popular scam methods such as text messages and automated phone calls to attempt to lure people into parting with personal or financial information.

Please remember:

- Never click on links in emails from unknown senders
- Beware of fraudsters using official-looking branding to make their emails appear legitimate
- Check the sender's details
- Report suspected phishing emails (forward the suspect email as an attachment to the internal spamreports@nhs.net account if your work email has been targeted, report@phishing.gov.uk if your personal email has been targeted)
- If in doubt, hang up/ignore the email and seek advice from your Local Counter Fraud Specialist or Action Fraud

## Staying Safe Outside Work

### Members of the Public Targeted by Covid-19 Vaccine Telephone Scam

There have been reports of vulnerable and elderly people being targeted by fraudsters offering access to the Covid-19 vaccine in exchange for a payment over the phone.

This is an evolution of the flu jab scam which we covered in previous newsletters. The fraudsters are now shifting from promising access to the flu jab at home, to trying to convince people that they can be "bumped up" the list or gain access the Covid-19 jab privately in exchange for payment.

This scam is designed purely to convince vulnerable people to part with their financial information.

The NHS are the only organisation with access to the vaccine and will not ask for a fee to be paid in order to access the jab.

If the person calling asks for a payment to be made, the call is not genuine and you should hang up the phone.

If a friend, family member or neighbour reports that they have made a payment for early access to the vaccine, they should be directed to contact Action Fraud (0300 123 2040) and to speak to their bank.

## Action Fraud Launches #FraudFreeXmas Campaign

Action Fraud is warning consumers to look out for deals that appear “too good to be true” during the Black Friday and festive shopping season.

Action Fraud figures show that reports of online shopping fraud have been 30% higher throughout the pandemic, as more people than ever are making purchases online.

Last year, the loss to shoppers during the run up to Christmas was almost £13.5 million. Action Fraud are advising everyone to be careful about where they shop (research first, including checking reviews and seller history), how they pay (use payment methods that carry consumer protection such as credit cards or PayPal) and to look out for phishing emails.

You can read more about the campaign on the Action Fraud website by clicking here

## Royal Mail/DPD “Missed Parcel” Scam

In the period between Black Friday and the January sales, it can be really easy to lose track of which parcels are coming to your address, and who will be delivering them.

Fraudsters are taking advantage of this busy shopping period by renewing their efforts to carry out parcel delivery scams. At the moment, fraudsters appear to be impersonating the Royal Mail and DPD, but it is likely they will diversify to include other major parcel delivery companies.

This scam works when you receive an email to let you know that a parcel delivery attempt was made but could not be completed. The message will ask you to click on a link to schedule a second delivery attempt.

If you click on the link, you will be diverted to a phishing site where you will be asked to enter personal data such as your full name, date of birth, address, phone number and bank details.

You should be very careful if you receive any emails of this nature. Check the sender’s email address to see if it has come from an official account, and consider contacting the delivery company using their official customer service contact details. Be especially wary of text messages following this format too, as it is easy for fraudsters to disguise their details by placing a label “e.g. RoyalMailUK” over their real number, and which will be displayed when they text you.

You may find it helpful to keep a note of any orders you place along with the delivery method/tracking numbers which will be used. If in doubt, do not click on any links within suspicious emails, and report them to the National Cyber Security Centre via their dedicated email address: report@phishing.gov.uk

## Food Bank Fraud

Unfortunately, fraudsters will use any tactic they can think of to part people from their money. There have been local reports of a member of the public being targeted over social media.

The individual was a regular attendee at a food bank. They received numerous friend requests from someone they did not recognise, but who shared a mutual friend with them. The friend request was accepted, and the new friend sent a link through, claiming that in order to collect their next food parcel they needed to provide personal and financial information.

The person complied with this request, and their bank account was emptied. Please be aware of this scam, and if you or anyone you know is accessing support from a food bank, please do share this information with them.

## Action Fraud Charity Fraud Warning

At this time of year, many people chose to donate to charity. Unfortunately, fraudsters are also happy to impersonate genuine charities, or to set up fake charities in order to target donations being made.

Action Fraud reports that last year, £350 million of charitable donations made during the festive period ended up lining the bank accounts of criminals. Although the majority of appeals for donations are genuine, fraudsters will always look for opportunities to defraud the public using national and global events as a front. Action Fraud reported earlier this year that it had received reports of a scam email, purporting to be from HM Government, asking for donations to the NHS as part of a ‘nationwide appeal in efforts against coronavirus’.

This year, Action Fraud has teamed up with the Charity Commission and the Fundraising Regulator to provide advice and support to allow you to donate with confidence.

You can find more information about safely donating to charity by visiting the Gov.uk website here: https://www.gov.uk/government/news/donate-your-money-to-charities-not-criminals-this-christmas

## Counter Fraud Training

### Training Sessions

A central part of your Local Counter Fraud Specialist's role is to raise awareness of fraud within the NHS. This can take many forms but the most successful and popular method for us to do this is via face-to-face training with staff. Thanks to the range of conference calling software now at most people's fingertips, we're able to offer online fraud training.

Our Fraud Awareness training focuses on:

- How different types of fraud affect the NHS
- Practical advice on what to look out for and methods to protect yourself and your organisation from fraud
- Real life case studies showing how the NHS is targeted
- Information on how to report concerns about fraud

This training can be arranged to suit you and will be delivered via Microsoft Teams. It is part of our normal service and can be delivered to groups of any size. We are also able to design and deliver bespoke training packages based on any fraud related areas of concern that you feel are most relevant for your team.

We are currently running a series of mandate fraud and phishing refresher training sessions via Teams. If you are interested in accessing this training, or to discuss other fraud training requirements, please contact the LCFS team using the details below.

We are also offering out refresher training for any staff who are responsible for carrying out pre-employment checks for new starters. The pandemic has changed how and when identity documents and qualification certificates are presented. The refresher training provides advice on what to look out for. To register your interest in a session, contact one of the LCFS team using the details below.

## How to Contact your Local Counter Fraud Specialist

If you would like more information or advice about fraud and the latest scams, or to raise a concern please feel free to contact your Local Counter Fraud Specialist. You can find our contact details below:


| | |
|---|---|
| Steve Moss, Head of Anti-Crime Services | Steven.moss@nhs.net<br>07717 356 707 |
| Marie Hall, Assistant Anti-Crime Manager | Marie.Hall15@nhs.net<br>07970 265 017 |
| Rosie Dickinson, Local Counter Fraud Specialist | Rosie.dickinson1@nhs.net<br>07825 228 175 |
| Lee Swift, Local Counter Fraud Specialist | Lee.Swift1@nhs.net<br>07825 110 432 |
| Shaun Fleming, Local Counter Fraud Specialist | Shaunfleming@nhs.net<br>07970 264 857 / 07484 243 063 |
| Adele Jowett, Associate Local Counter Fraud Specialist | adele.jowett@nhs.net<br>07970 264 951 |
| Nikki Cooper, Local Counter Fraud Specialist | Nikki.cooper1@nhs.net<br>07872 988 939 |
| Richard Maw, Trainee Anti Crime Specialist | R.maw@nhs.net<br>07771 390544 |