DECEMBER 2023

AUDIT YORKSHIRE

# COUNTER FRAUD NEWSLETTER

Welcome to our December 2023 Counter Fraud newsletter for NHS staff. We hope you find the contents helpful. If you need any advice on fighting NHS fraud, you can find our contact details on the final page.

## IN THIS EDITION



**Money Laundering - What is it?**

It is exactly what it says on the tin – a way to make criminal money 'clean'. This is often done through a series of transactions so that anybody investigating it will hopefully lose the trail. It's usually done in three stages:

**Placement** – introducing the 'dirty money' into financial systems
**Layering** – lots of transactions to hide the source of the money
**Integration** – the clean money can be withdrawn and used. A background check will show that it has come from a legitimate source.

Criminals looking to clean their money may try and recruit you to help them. Some will advertise jobs which involve moving money around, others may try and befriend you before asking for "a favour". They will ask you to receive a transfer or to pay cash into your account, before you move it on elsewhere. As an incentive they are likely to offer you a cut of the money or gifts in exchange.

A criminal is unlikely to tell you the real reason for needing your help – they will probably give you a cover story or excuse why they can't accept the money into their own bank account at the moment.

If you do move money on their behalf, you may be committing a criminal offence with a potential maximum sentence of 14 years. You may also have your bank account closed and could struggle to get a new one. Getting credit such as student loans, phone contracts and a mortgage can also prove very difficult. There is a very helpful article on the Barclays website that explains more.

Recent press articles have highlighted an increase in organised criminals trying to entice students into acting as money mules, and another notes that the cost of living crisis has led to more middle-aged people agreeing to be involved.

Please be vigilant if anybody approaches you with an offer which seems to good to be true. Being involved in money laundering is a criminal activity. Don't fall for the offers of a return in exchange for using your bank account.

# Scam Trends and Fraud News


**Top Ten Fraud Types 2023**

As we come to the end of the year, it's time for a classic Top Ten! Natwest recently commissioned a study which has revealed the top ten most common frauds in 2023.

It found that 13% of all British citizen's have lost money to fraud, with 7% losing as much as £5,000. You can read their full article here. It's worth remembering that fraud tends to be under reported, so the true amount of fraud is likely to be even higher than these figures suggest.

1. **Phishing Scams** (37% of the British public targeted) - Fake emails, calls, messages or websites that seem to be from legitimate organisations, and which ask you to provide personal/financial information.

2. **Trusted Organisation Scams** (21%) Fraudsters impersonate trusted organisations such as the HMRC, energy companies or service providers. They claim there is an issue with your account, or that you owe a fine etc.

3. **Refund Scams** (13%) Fraudsters impersonate trusted organisations and claim that you are due a refund. This is about getting you to share personal or banking information. Instead of getting a refund your details are stolen.

4. **Friend or Family Scams** (12%) Messages sent to your phone or via social media claiming to be from someone you know. They ask you to send them money to help pay an unexpected bill or to help with an emergency.

5. **Get Rich Quick Scams** (9%) Fraudsters claim you will make money quickly by investing in a company or goods, and promise huge profits. This can be tempting with cost of living pressures. Remember: if it seems too good to be true, then it is!

6. **Purchase Scams** (9%) Criminals place adverts for fake goods and products online, on social media and auction sites to gain money or information. Products often include games consoles, concert tickets, and even holidays.

7. **Investment Scams** (8%) Fraudsters encourage people to invest money into fake opportunities or pyramid schemes.

8. **Safe Account Scams** (7%) Criminals pretend to be calling from your bank or the police and claim there has been fraudulent activity on your account. To "protect the funds" you are asked to move money to a new account.

9. **Lottery Cons** (7%) Fraudsters claim you have won a lottery prize. and ask for your financial information so they can send you your "winnings".

10. **Befriending Scams** (6%) Fraudsters use a false identity to build up a friendship before asking for money, login information or other favours.

**Fake community pharmacy calls**

The Counter Fraud Team have heard about fraudsters who have phoned patients, pretending to be from a community pharmacy.

The caller has said they are ringing to arrange the delivery of medication, but have asked the patient to confirm their full name, date of birth, address and some banking details.

Fraudsters can be very convincing and so we ask that if you have any vulnerable friends or relatives, you let them know about this scam. They should be particularly mindful of such calls if they do not usually pay for a prescription medication service.

We recommend that if such an unsolicited call is received, that the patients hangs up and contacts their pharmacy as they usually would. We advise that either a different phone is used, or to wait for a period of at least 20 minutes before making any verification phone calls just in case the fraudster has jammed the line.

Patients can find out more information to protect themselves from fraudsters by visiting the Action Fraud website.

# Cyber Fraud

## Social Media Shopping Scams

In the run up to the festive period, many of us will be on the hunt for the perfect gift at the best price. Fraudsters are aware of the most popular gifts that people are looking for, and set up listings on social media market places for these items.

As the festive season gets closer and items go out of stock at established retailers, the pressure to take a gamble on a social media listing can become intense.

**Fake Items for Sale**

Fraudsters can ramp up the pressure by offering expensive goods for bargain prices. To test out how quickly a fraudster can set up a fake listing, This Is Money created a fake profile on Facebook and listed a £770 phone for sale at £250. Within 24 hours, more than 827 people had looked to buy the smartphone. Of those, 16 had offered to make payment. When they were told the phone had already been sold, many stepped up their offers asking if there was any way they could get the deal.

- Please be very cautious if you see items listed for sale that are too good to be true.
- We would normally advise to check the sellers profile to see if they are new to the social media platform, but fraudsters are wise to this advice and now often hijack real profiles to use for scamming others.
- Do not pay by bank transfer in advance - the person may vanish and delete their profile once you have sent payment.
- Look out for pressure tactics such as being told that the seller has had lots of offers.

**Fake Purchase Requests**

Not only did a high number of genuine customers get in touch, but so did lots of fraudulent accounts wanting to "buy" the phone.

- If you are selling anything on social media, please be very wary about offers where the potential purchaser wants to arrange for a courier to collect the item and drop off a cash payment. If you agree the fraudster will say that the courier requires an additional insurance policy. The scammer will suggest as they've paid for the collection, that you pay for the insurance - and then send you a link which will harvest your payment details.

You can read more about the experiment that This is Money ran on their website.

**Online Fraud Charter**

Regular readers of the newsletter will probably have noticed that we've written a lot of articles about social media fraud in the past few years. Fraud is the most common offence in the UK, accounting for over 40% of crime.

Those committing fraud often do so online as it's much harder for the victim to identify who has defrauded them. A fraudster can hijack someone else's account, or create a fake profile from which to target others.

On the 30th of November, a host of leading tech companies met with the UK Government to sign a first-of-its-kind Online Fraud Charter. Companies who signed up include Google, Facebook, Instagram, eBay, Amazon, LinkedIn, Microsoft, Match Group, X (Twitter), Tik Tok and YouTube.

Those signing up are committing to taking action to prevent fraud. Examples include verifying new advertisers, increased verification for peer-to-peer marketplaces (such as eBay, AirBNB and Amazon), and offering dating site users the ability to verify their own identity.

In addition to clamping down on scam posts, each signatory has pledged to work closely with the police in their efforts to target fraudsters, including direct routes for law enforcement to report suspicious activity taking place on the services. The goal is to make it easier to quickly identify and remove fraudulent content and protect users.

You can read more on the GOV.UK website, where you can also read the Online Fraud Charter in full.

# The Spell

THE PSYCHOLOGY OF FRAUD

Scammers are often masters of deception, with a range of tools to help them get past our defences. They use social engineering and coaching tactics to put victims under what is becoming known as 'The Spell'.

Victims who are drawn into The Spell will be so convinced by what they are being told that they will lie to their banks, the police, and even their friends and family if they are questioned.

Some banks have Break The Spell Teams. They monitor unusual payments and speak to customers to make sure they are not being scammed. Millions of pounds have been prevented from being sent to scammers by these teams. However, the staff on these teams are often met with aggression and abuse because the victims have been coached to lie to the banks.

When we read about fraud in the cold light of day with all the facts laid out, no emotional investment, and the full benefit of hindsight, it is easy to see which strings have been pulled. However, the victim will have seen it very differently from the inside. We always advise not to give data away if you don't trust somebody. However, whilst they are under The Spell, victims **do** trust the people that are exploiting them.

It's no wonder that 40% of all crime is fraud when we see how vulnerable we are to coercion.

Fraud can be very similar to marketing, pressing the same buttons that make us keen to snap up a bargain. The engineers behind a fraud attempt want you to take action whether this is through excitement, hope, fear or another emotion.

So how do the scammers manage to put rationally thinking, intelligent people under The Spell?

**Flawed Risk Assessments**

Human beings are actually quite poor at assessing risk unless there is an emotional or visual connection to that risk.

Some people are scared of flying. Statistically, we are way more likely to be in a car accident than a plane crash. However, few people arrive at an airport by car feeling thankful that the most dangerous leg of their journey is over. The image of a plane crash is much more impactive to most people than a car accident, and so we attach a higher risk to it.

Do you have a mental image for what fraud looks and feels like? Unless you or one of your loved ones has been a victim, you probably don't have an image which pops into your head when you hear the word "fraud".

There is often no emotional hook. Humans are therefore not motivated by the risk of fraud. In contrast, being offered an amazing investment opportunity or thinking you have found the love of your life does have a strong emotional pull, and we may think the risk is worth it.

**Unprotected Personal Data**

Add to this biased risk assessment that humans like to touch, see and feel things. As we can't do this with our data, we don't protect it like we would our tangible possessions. It's also easier to make an online payment than to part with cold hard cash, especially now that many of us have our card details saved into our phones.

**Technology**

Our closest connections used to be people - whether this was family, friends or workmates.
We now have an extremely strong connection to technology.

We also have confirmation-bias - we only see what we want to see. If a fraudster tells us we will make money, and this is what we want to hear, we will be inclined to believe them. This makes us vulnerable to manipulation.

We also tend to read what supports our view and selectively research to find evidence that supports what we already want to believe. We can ignore or excuse any negative feedback until we are a victim.

## Articles about The Spell

**Nurses targeted by crypto-scam**
When two retired nurses were caught up in an investment scam, fraudsters used The Spell to take over £86k. Read more about this story on the BBC website.

**Cruel romance scam led to £70k loss**
The story of a 56 year old lady who was fleeced by a romance scam. This article also talks about the work of the Break the Spell team at Santander. You can read the full article on the ITV website.

**On the next page you'll find some advice on avoiding falling under The Spell...**

## Breaking The Spell

Removing the emotional blind spot that fraud tends to sit in is a great first step. It is useful to understand that this is how the fraudsters try to manipulate you, so that you can properly risk assess situations.

Speak to people rather than relying on research online - your friends, family, and your bank can all help you.

If you are asked to lie to your bank, take this as a significant warning flag.

Remember, the person who has promised you a "sound investment" and tells you what to say to your bank is going to be the person who receives your money.

The banks who question you about what a transfer is for will not be gaining anything. Their only interest is to keep you safe. If you do lie to a bank and it turns out you are the victim of a fraud, they may not refund you.

Think of your personal information as a possession. You wouldn't give your car or house keys to a stranger so definitely don't give a stranger your address, date of birth, bank details etc.

Don't let yourself be panicked or rushed into making a decision. Take a break before sending money anywhere, and if in doubt speak to your bank.

# Fraud Prevention Masterclasses

The 2023/24 Fraud Prevention Masterclass programme is underway. The Masterclasses are delivered via Microsoft Teams and sessions typically last around 1 hour. Further dates will be published later this year. We will be covering the following topics:

| | |
|---|---|
| General Fraud Awareness | 6th February 10:30am |
| Fraud Awareness for Managers | 16th January 11am |
| Cyber Fraud | 7th February 11am |
| Payroll Fraud | 23rd January 10am |
| Procurement Fraud | 15th February 2pm |
| Creditor Payment Fraud | 16th January 10am, 12th March 2pm |
| Fraud Awareness for HR | 20th February 10am |
| Recruitment Fraud | 16th January 10am, 12th March 11am |

If you would like to book a place for any of these sessions, please contact yhs-tr.audityorkshire@nhs.net

**Bespoke Training Sessions**

The Local Counter Fraud Team are always happy to pop along to speak to individual teams. If you would like us to attend one of your team meetings, to deliver a training session on a key fraud risk area, or for any other fraud prevention advice, please contact us using our details (which you'll find on the last page).

# REPORTING FRAUD CONCERNS

## Fraud vs the NHS

If you think that fraud may be being carried out against the NHS, please **notify your Local Counter Fraud Specialist**. You'll find our contact details on the next page.

You can also report your concerns to the **NHS Counter Fraud Authority** using their online reporting tool or phone number. You'll find these details on the next page.

If you choose to make an anonymous report, please give as much information as possible as we won't be able to get back in touch with you to clarify anything.

## Suspicious Emails

**Do not click on any links or attachments**.

If you have received a suspicious email to your **@nhs.net** email account, you can forward it (as an attachment) to **spamreports@nhs.net**

If you are not sure how to forward an email as an attachment, contact the LCFS team and we will help you.

If you have been sent a suspicious email to another type of email account (not @nhs.net) you can forward it to **report@phishing.gov.uk**

## Suspicious texts

Do not click on any links in the suspicious text message.

You can forward suspect text messages to 7726.

## Fraud against a member of the public

These concerns can be reported to **Action Fraud (0300 123 20 40),**

If the person has lost money, it may also be appropriate to report the matter to **the police.**

If you suspect that the person's bank account has been compromised, it is important that they **speak to their bank** as a matter of urgency.

## I've read the options but I'm still not sure what to do

The Local Counter Fraud team will be happy to advise.

Our contact details are on the next page.

# CONTACT US

**Acronym Decoder**
LCFS - Local Counter Fraud Specialist
LSMS - Local Security Management Specialist
ICB - Integrated Care Board


**Steve Moss**
Steven.Moss@nhs.net / 07717 356 707

**Head of Anti Crime Services / LCFS**

Steve manages the Counter Fraud Team.

**Marie Dennis (was Hall)**
Marie.Dennis2@nhs.net / 07970 265 017

**Assistant Anti Crime Manager covering all clients, and LCFS covering:**

York and Scarborough Teaching Hospitals NHS Foundation Trust

NHS Professionals

**Nikki Cooper**
Nikki.Cooper1@nhs.net / 07872 988 939

**LCFS Covering:**
Humber Teaching NHS Foundation Trust

Humber and North Yorkshire ICB

Leeds Community Healthcare

**Rosie Dickinson**
rosie.dickinson1@nhs.net / 07825 228 175

**LCFS Covering:**
Harrogate and District NHS Foundation Trust

Spectrum Community Health CIC

West Yorkshire ICB

**Shaun Fleming**
ShaunFleming@nhs.net / 07484 243 063

**LCFS and LSMS Covering:**

Calderdale and Huddersfield NHS Foundation Trust

West Yorkshire ICB

Lincolnshire ICB

**Rich Maw**
R.Maw@nhs.net / 07771 390 544

**LCFS Covering:**

Bradford Teaching Hospitals NHS Foundation Trust

Local Care Direct

Mid Yorkshire Teaching NHS Trust

**Lee Swift**
Lee.Swift1@nhs.net 07825 110 432

**LCFS Covering:**
Airedale NHS Foundation Trust
AGH Solutions
Bradford District Care NHS Foundation Trust
Leeds and York Partnership NHS Foundation Trust


You can also report fraud concerns to the NHS Counter Fraud Authority:
0800 028 40 60
https://cfa.nhs.uk/reportfraud

Follow us on Twitter - search for @AYCounter Fraud

Scan here to see previous editions of our newsletters