

Student guide to

FRAUD



C Contents

02 Contents

03 Money Muling

04 Online Shopping Fraud

05 Parcel and Ticket Fraud

06 Accommodation Fraud

07 Employment Fraud

08 International Students

09 Romance Fraud and Sextortion

10 How to Report



Money Muling

Money Muling is the laundering of the proceeds of crime which is disguised by criminals as a way for you to make money. It helps to fund serious and organised crime.

A Money Mule is someone who enters this business relationship. They let someone else use their bank account to transfer money in return for financial reward.

This is a crime. If you enter into this type of business relationship you are committing a crime which carries a maximum prison sentence of 14 years.

- You could get a criminal record.
- You could have all your bank accounts and credit channels frozen.
- You could be discharged from your education provider.
- You are putting yourself and people you know in danger.

Professor Nicholas Ryder - Financial Crime expert

"Fraud is the funding mechanism of choice for organised crime and terrorist groups, who rely on laundering their money or using alternative banking methods to avoid police."



Signs

- Too good to be true
- Unsolicited contact
- Unsolicited job offers
- No experience required
- Earn from home
- Get rich quick offers
- Request for your bank account details
- Easy money with no strings attached
- Requests to transfer money
- Requests for your bank account details



Advice

- Stop and think
- Consult with trusted people
- Question unsolicited job offers
- Question job offers from overseas
- Look for poor spelling and grammar
- Research companies to make sure they are genuine
- Protect your personal and financial information
- Keep your bank account details secure and private
- Never transfer money on behalf of someone else

Online shopping fraud

Online Shopping Fraud is when criminals create fraudulent shopping scams to exploit consumers during online shopping and auctions.

The criminals use the secrecy of the internet to establish the deception, creating cloned websites with URL alterations. They may also ask for payment prior to delivery and send you fake receipts and invoices.

Criminals will offer goods for sale that you will not receive, they will market products at low prices to attract customers, persuade them to make payment through direct bank transfers, and vanish once the payment is made.

As buyers they will purchase goods from you but not complete the payment. There are numerous methods of achieving this including overpayment, fake banking APPS, direct payment away from the online marketplace and denial they received the goods as promised.

Online Shopping Fraud is connected to many other types of Fraud including Parcel Fraud and Ticket Fraud.



Signs

- Too good to be true
- Unsolicited Contact
- Goods offered at a bargain price
- Offers of further discount
- Requests payment by bank transfer
- Check spelling and grammar
- Check every character in address bar, email addresses and domain names
- Seller applies pressure for payment
- Look for a padlock icon in the address bar – if there is not one then leave the site – if there is one, it may still be fake
- Lack of Privacy Policy and/or Returns Policy
- Recently opened website
- Promise that customer representative will meet you at the venue

Professor Nicholas Ryder - Financial Crime expert

"It has been estimated that the cost of fraud in the UK exceeds £200bn per year, 86% of fraud is unreported, over 70% of fraud has an international element and it costs the global economy £4.4tn."

Parcel Fraud

Parcel Fraud is when criminals contact victims by email, social media, phone and post trying to trick them into thinking a parcel needs to be delivered.

Criminals also pose as police or customs officials claiming you are under investigation for the contents of a parcel.

Even if you are expecting a parcel NEVER use the contact details provided by them.

Ticket Fraud

Common Ticket Fraud targets are major sporting events, summer festivals and big-name arena and stadium performers.

Fraudsters create fake websites and social media profiles to sell tickets that are fraudulent or non-existent.

They will offer tickets before the real tickets have been released and when events have sold out.



Advice

- Stop and think
- Consult with trusted people
- Check the sites contact details / geographical address
- Check Companies House www.gov.uk
- Read Reviews
- Check for clone/copycat sites
- Pay with a credit card
- Avoid bank transfers
- Go directly to genuine websites Do not use links
- Protect your personal and financial information
- Book through official sellers



Accommodation Fraud

Accommodation Fraud is when the criminal tricks you into sending money for a room which doesn't exist or belongs to someone else.

Fraudsters use a variety of websites and social media platforms to advertise properties, often at attractive costs and in desirable locations.

The offers will appear professional and genuine, accompanied by the expected photos, reviews and contact information.

Due to high demand for accommodation, the fraudster will apply pressure and victims will often be asked pre-viewing, to pay upfront fees in order to secure the property.

The fraudster will use sophisticated methods to trick you into believing they are genuine.

They will often not have ownership of the properties they are advertising.



Signs

- Cheap room/s
- Basic websites
- Basic social media accounts
- Contact requested privately away from platform
- Poor photos, spelling and grammar
- Request to use money transfer service
- Apply pressure for you to act quickly



Advice

- Stop and think
- Consult with trusted people
- Check websites contact details / geographical addresses
- Check Companies House www.gov.uk
- Check for clone/copycat sites
- Reverse Image Search accommodation photos
- View in person
- Check if the landlord is registered

Employment Fraud

Employment Fraud happens when a fraudster claims to be a recruitment agent or employer, offering to hire you for a job which doesn't exist.

Fraudsters send unsolicited messages, letters, phone calls and emails claiming to be in a position to offer work.

They often use questionnaires to obtain personal information which they can use to commit further crimes.

The fraudsters will ask for your bank account details under the guise of setting up salary payments. They can use these details to steal money from the account and commit further crimes.

They may even ask you for fees during the application process. No reputable employer will ask you for a fee.

Professor Nicholas Ryder - Financial Crime expert

"The unprecedented and evolving threat presented by fraud has not changed. Fraud represents a large proportion of all reported crime each year in the UK."



Signs

- Unsolicited contact
- Questionnaire
- Request contact privately away from platform
- Poor spelling and grammar
- Request fees during application process
- Request to use money transfer service
- Request for bank account details
- Apply pressure for you to act quickly



Advice

- Stop and think
- Consult with trusted people
- Check websites contact details / geographical addresses
- Check Companies House www.gov.uk
- Check for clone/copycat sites
- Check email addresses and names online
- DBS checking service for legitimacy of company requesting DBS fees
- Use www.jobaware.co.uk and www.which.co.uk

I nternational Students

Certain types of fraud target international students.

Criminals sometimes impersonate organisations like the Police or Border Force and contact people stating they are part of an investigation, making threats of deportation if they do not pay a large sum of money.

Parents should be aware that they could be contacted with fake kidnap threats, stating their child has been kidnapped and they require payment before they are released.

Be wary when using group chats with unknown group members, sometimes these are used to communicate with individuals outside the chat.

They may make offers of cheap currency exchange or other services.

Professor Nicholas Ryder - Financial Crime expert

"Universities, their staff and students are regularly exposed to possible fraud and involvement in criminal activities and are at risk of criminal and civil liability for committing money laundering and fraud."



Signs

- Unsolicited contact
- Request to use money transfer service
- Request for bank account details
- Apply pressure for you to act quickly
- Request large sums of money



Advice

- Stop and think
- Consult with trusted people
- Do not transfer any money
- Do not give out personal or financial information



Romance Fraud

Romance Fraud happens when a criminal contacts you, most likely online using social media, chat rooms or dating apps. They form an online relationship by manipulating the person they are communicating with into thinking they are friends or a romantic relationship.

Once the criminal has established the relationship, they will ask the victim to send money, often providing a story to make the victim sympathise with a fictional situation. This could be a health scare, subsidies until wages are paid or travel costs.

Sextortion

Sextortion happens when someone contacts the victim, most often using social media or dating apps and requests the person sends them sexually explicit images or videos.

They then threaten the person stating they will share the content unless they pay.



Signs

- Unsolicited contact
- Request contact privately away from platform
- Poor spelling and grammar
- Is trying to establish a relationship very quickly
- Sends you sexual images or videos first
- Request for bank account details
- Apply pressure for you to act quickly



Advice

- Stop and think
- Consult with trusted people
- Cut contact immediately and block the user
- Do not pay any money and do not send any further images or videos
- Save the messages and report to the police

Professor Nicholas Ryder - Financial Crime expert

"Fraudsters will use a variety of techniques via every social media platform. Stay wise and stay alert for scammers."

How to report



Police

All fraud in the UK is reported to the police at Report Fraud by phone or online: **0300 123 2040**
www.reportfraud.police.uk

Report Fraud is the central reporting point for all reports of fraud, your local police force will be informed by Report Fraud.



Emails

Forward fraudulent emails to
report@phishing.gov.uk



Banks

Dial 159 (Stop Scams UK Anti-Fraud Hotline) An automated line which takes you through to your bank's fraud team.

For alternative ways of contacting your bank only use the contact details on your bank card or the official website.



Phone Numbers

Forward phone numbers sending you fraudulent messages or calls to **7726**

Visit our NWROCU website for more information by scanning the QR code below.



Student guide to

FRAUD

Developed by the RECCC at NEROCU in collaboration with Financial Crime expert, Professor Nicholas Ryder.