Key threat – money mules

Don’t be Fooled campaign, supported by Barclays

Don’t Be Fooled is a partnership between Financial Fraud Action UK (FFA) and Cifas. It aims to deter students from becoming money mules, by educating them about what the term means, how criminals operate and why they are a target.

In Barclays, 52% of money mules are 25 or under and the majority of those are between 17-21 years old.

The national fraud reporting service Action Fraud receives up to 70 calls a week from people worried that they may unwittingly have become mules. There are serious consequences of participating in such schemes.

Students need to be aware of the long term consequences of becoming a money mule.

More about fraudsters tactics:
Barclays.co.uk/security/how-fraudsters-make-contact/

Students fraud safety:
barclays.co.uk/journal/stay-fraud-smart-at-uni/

Go to moneymules.co.uk to find out more.

What is a money mule?

A money mule is someone who is asked by a third party to receive money into their bank account and transfer it onto another account, or allows a third party to take control of their account. The money being transferred is the proceeds of crime.

A money mule is involved in money laundering, which is a crime. Not knowing that it's a crime is no excuse, so account-holders could still be prosecuted.

The organised criminal gangs behind money mules often use the proceeds of crime to commit other serious offences such as drug, people trafficking and terrorism.

People that are recruited as money mules can be threatened with violence or physically attacked if they do not continue to let their account be used to transfer money.

Criminals often pose as employers, targeting young people on social media but sometimes target banking staff.

People often become money mules unwittingly. They might think they're giving out their bank details for a genuine reason, then end up involved in money mule fraud.

What should you do if a customer comes in saying they might have been a victim?
If a student realises they are a victim, they must report this to the bank and the police immediately.
Keeping students safe

What happens when they are caught?

Barclays has sophisticated systems in place to detect suspicious money moving across accounts. We report this to the authorities through our SAR/1370 form reporting process.

When a money mule is caught, their bank account will be closed making it hard to get student loans, mobile phone contracts or other access to credit. It could also damage their job prospects and if prosecuted, can result in a prison sentence for up to 14 years.

Why are students targeted?

Students pose a great opportunity for fraudsters, as they’re often short of cash, but the same could be true of a single parents juggling lower incomes. International students who are using a bank account for a limited time can be enticed to sell their accounts on.

For many students, it is the first time they have left home and have to budget and take control of their own finances. Some don’t realise the severe consequences and risks involved and don’t think they will get caught. The fraudsters will make up compelling stories. When the mule is caught, the fraudster will suddenly vanish.

Give this advice to student customers:

• Don’t give your bank account details to anyone unless you trust them and you know exactly where the funds have come from.
• Be cautious of unsolicited offers of easy money. If it sounds too good to be true, it probably is.
• Research any company that makes you a job offer and make sure their contact details are genuine.
• Be wary of job offers from overseas. It will be harder for you to find out if they are legitimate.
• Be wary of job ads that are written in poor English, with grammatical errors and spelling mistakes.
Being more fraud aware at Uni

Fraudsters can take advantage of university students – learn how to help them protect themselves with our handy tips

Whether it’s via a smartphone, laptop or other digital device, they always connected – for the serious (study and revision!) as well as social activity, and for the most part, it’s great! Unfortunately, it also exposes them to the threat of fraud and scams. Here are some to watch out for and how students can protect themselves.

‘Phishing’
Fraudsters send emails (often appearing to be from the student’s bank or an official body such as HMRC) asking them to disclose personal information or send money. They may also ask them to download a file or click on a link to a bogus website, which then allows fraudsters to access their details.

What they can do
Don’t click on any links or open any attachments from unsolicited emails. Make sure their anti-virus software is up to date and if they receive a suspicious email from their bank let them know (details of how to do this should be on your banks website). If they are unsure they can check your banks website to see what they will and won't ask them for in an email. Banks will never ask them to transfer money to another account.

‘Vishing’
They may receive a phone call out of the blue from someone claiming to be a bank fraud prevention officer or an officer in technical support from a company’s customer services. The pitch may then go like this: they’re calling about a refund or problem with their payment card. To sort it, they ask them to confirm security and bank account details. When these are shared the fraudsters then take payments from the account.

Or another possible scenario is tech support impersonators claim they’ve detected a fault with the student’s laptop or computer and need to access it remotely to fix the problem. They may also say they need to buy a piece of software straightaway to solve the problem.

What they can do
Such a call out of the blue is unlikely to be legitimate, so if they’re unsure of the person’s credibility, hang up. Go online and find the number for the relevant company/department they’re claiming to be from. If possible, call them from another phone as fraudsters can keep the line open, that way they can be confident they’re speaking to a legitimate person from the company or organisation they have a relationship with.

Online shopping scams
It’s never been easier to book tickets for gigs, grab a student discount for dinner or buy books for courses online. Unfortunately, this also makes it easy for fraudsters to advertise fake products or a bogus service, and take the student’s money, but then never deliver what they paid for.

What they can do
Before sending your cash to a private seller or even a legitimate-looking brand research the seller and review their feedback. Never follow a link in an unexpected email. It’s also a good idea to check the spelling in the URL to make sure it’s legitimate. As an example, barclays-bank.co.uk is incorrect – the real URL is barclays.co.uk. Insist on seeing high-value items like vehicles before paying, and always use secure payment methods rather than direct bank transfers.
Keeping students safe

Don’t be Fooled campaign, supported by Barclays

Don’t Be Fooled is a partnership between Financial Fraud Action UK (FFA) and Cifas. It aims to deter students from becoming money mules, by educating them about what the term means, how criminals operate and why they are a target.

What is a money mule?
A money mule is someone who is asked by a third party to receive money into their bank account and transfer it onto another account, or allows a third party to take control of their account. The money being transferred is the proceeds of crime.

A money mule is involved in money laundering, which is a crime. Not knowing that it’s a crime is no excuse, so account-holders could still be prosecuted.

The organised criminal gangs behind money mules often use the proceeds of crime to commit other serious offences such as drug, people trafficking and terrorism.

People that are recruited as money mules can be threatened with violence or physically attacked if they do not continue to let their account be used to transfer money.

Criminals often pose as employers, targeting young people on social media.

People often become money mules unwittingly. They might think they’re giving out their bank details for a genuine reason, then end up involved in money mule fraud.

Resources:

More about fraudsters tactics:
Barclays.co.uk/security/how-fraudsters-make-contact/

Students fraud safety: barclays.co.uk/journal/stay-fraud-smart-at-uni/

Go to moneymules.co.uk to find out more.

What happens when they are caught?
Barclays has sophisticated systems in place to detect suspicious money moving across accounts. We report this to the authorities through the suspicious activity reporting process.

When a money mule is caught, their bank account will be closed making it hard to get student loans, mobile phone contracts or other access to credit. It could also damage their job prospects and if prosecuted, can result in a prison sentence for up to 14 years.

Why are students targeted?
Students pose a great opportunity for fraudsters, as they’re often short of cash, but the same could be true of a single parents juggling lower incomes.

International students who are using a bank account for a limited time can be enticed to sell their accounts on.

For many students, it is the first time they have left home and have to budget and take control of their own finances. Some don’t realise the severe consequences and risks involved and don’t think they will get caught.

The fraudsters will make up compelling stories. When the mule is caught, the fraudster will suddenly vanish.

Give this advice to students:
• Don’t give your bank account details to anyone unless you trust them and you know exactly where the funds have come from.
• Be cautious of unsolicited offers of easy money. If it sounds too good to be true, it probably is.
• Research any company that makes you a job offer and make sure their contact details are genuine.
• Be wary of job offers from overseas. It will be harder for you to find out if they are legitimate.
• Be wary of job ads that are written in poor English, with grammatical errors and spelling mistakes.

Been a victim?
If a student realises they are a victim, they must report this to their bank and the police immediately.