PRESS RELEASE

LLOYDS BANK

More young people being duped into ‘safe’ account scams

- **Four-fold increase in millennials who have fallen victim to impersonation scams**
- **Victims aged over 55 losing four times as much cash (£10k)**
- **Lloyds Bank unveils new campaign to crackdown on ‘safe’ account scams**

More millennials are falling victim to scams designed to trick them into handing over cash to fraudsters than any other age group, according to new data from Lloyds Bank.

There has been just under a four-fold increase in the number of 18-34 year-olds being caught out by impersonation scams in the past 12 months,* who are now as likely as those aged over 55 to fall victim to such scams.

Victims aged 18-34 are losing **£2,630** on average to these scams – while over 55s are losing more than four times as much per scam **(£10,716** on average), despite less of an increase in occurrence. Those in between (45-54) are being tricked out of **£3,573** on average, while there are also more than three times as many people falling victim in this age group.

Impersonation scams most often involve someone pretending to be from the police or a bank who may ask people to quickly transfer money into a ‘safe’ account. They often say that the police suspect the person’s account is in danger or that there is a problem with their bank.

Warnings from banks can often go unheeded as fraudsters coach victims into believing that bank staff are ‘involved’ in the scam.

Lloyds Bank has launched a new multi-media campaign to crack down on scams, including a new TV advert – to be aired for the first time on Monday 2 September – reminding customers that it will never ask them to move money into another account.

Recent research from Lloyds Bank and YouGov found that one in four UK adults knew someone who had been duped by a fraudster, and one in 10 have fallen victim to a financial scam at some point in their lives. Meanwhile a third (33%) said they have been targeted by fraudsters but were able to put a stop to it.

Paul Davis, Retail Fraud Director at Lloyds Bank, said: “Helping to keep our customers’ money safe is our number one priority – being a victim of fraud can have devastating effects not just on people’s finances but also their lives.

“While we are working 24/7 behind the scenes to protect customers and millions of pounds have been frozen, every day fraudsters are trying to trick people into handing over their personal information like a PIN or password or transferring cash.

“Our new campaign will help people to recognise the signs by reminding them that we will never call

MEDIA CONTACTS

Kimberley Hamilton **kimberley.hamilton@lloydsbanking.com** 07557 257 298
Gregor Low **gregor.low@lloydsbanking.com** 07500 078 879

PRESS RELEASE

LLOYDS BANK

and ask them to move money to another account. The more we all know about spotting scams, the safer we will all be."

TIPS TO HELP STAY SAFE FROM SCAMS

- **Question any requests to share details or move money –** Your bank will never ask you to share your account details like user ID, password and memorable information. You should also be alert if your bank suddenly tells you to move your money or asks you to transfer funds to a new sort code and account number. Contact them immediately if you receive any requests of this nature.
- **Check for spelling mistakes –** Get into the habit of checking for minor spelling mistakes in the addresses of any emails you receive. For example: "Lloids Bank" instead of "Lloyds Bank".
- **Double check the sender is real –** If you receive an email from anyone asking you to make an urgent payment, always double check the request is real by speaking to them in person, or by calling them on the number you have saved.
- **Beware of unexpected emails –** Be cautious about opening any emails that you weren't expecting (even if you think you recognise the sender), and don't click on any links or attachments unless you are sure they are genuine. Also, watch out for spoof text messages which may look similar to genuine messages you receive from your bank and always call the bank on the number on the back of your card to check if you're unsure.
- **Use anti-virus software and stay up to date –** Always use anti-virus software to protect your devices and ensure you have downloaded the latest updates for your operating system.
- **Make sure your internet banking site looks normal –** Do not log on or key in codes from your card and reader if any of the website pages look strange or different as this may indicate a virus infection.

OTHER COMMON TYPES OF SCAMS

Invoice fraud
This is when a fraudster contacts your company posing as a genuine supplier and asks you to change the bank details you use to pay them. Scammers can investigate a business's invoice details quite easily to make their approach look more convincing. They often try to hack supplier's emails to make it look completely normal. Make sure to check directly with a real contact if you get one of these emails with a number you know, and check to make sure it is genuine.

Scammers pretending to be service providers like telephone companies, rogue traders and HMRC
Fraud over the phone is when a fraudster calls claiming they're from a trusted organisation. They can often fake the telephone number on the screen and do their research to find out some of your basic bank and personal details. Remember though, a genuine bank will **never** ask you for personal or financial details like your PIN number or full banking password (even by tapping it into your phone keypad). They will never ask you to login on your banking online while you are on the phone.

Courier fraud
This is when you're called by someone pretending to be from your bank or building society and convinced to tell them your card details over the phone. They arrange for a courier to pick up your card to take it away for evidence or to have it destroyed. A genuine bank or organisation will never contact you out of the blue to ask for your full card details, PIN, full password or to move money to another account.

Investment scams on social media e.g. Instagram 'too good to be true' opportunities
This is becoming a tactic used by more and more fraudsters as it is easy for them to pop up on your Instagram. They advertise schemes that promising high returns within 24 hours after an initial investment. After you've sent the first payment via bank transfer, they send you screenshots showing huge 'profits,' but when you go to cash in your investment, your money – and the fraudsters – have disappeared.

MEDIA CONTACTS

Kimberley Hamilton	**kimberley.hamilton@lloydsbanking.com**	07557 257 298
Gregor Low	**gregor.low@lloydsbanking.com**	07500 078 879

PRESS RELEASE

LLOYDS BANK

Romance scams
These often take place through online dating websites, but scammers may also use LinkedIn or other social media sites or even email to make contact. Scammers will go to great lengths to gain your interest and trust, such as sharing 'personal information' and even sending you gifts. They may take months to build the relationship and pretend to need money for some sort of personal emergency. They might also ask for money to pay for travel to come and visit.

How Lloyds Bank tackles fraud

- Lloyds Bank (part of Lloyds Banking Group) has a 24/7 team dedicated to protecting customers from fraud.
- Our branch and telephone banking colleagues are specially trained to identify signs that could indicate that a customer could be a victim of fraud.
- We launched a mule-hunting team to detect and stop money mules at the start of 2018. The team's mission is to stop the movement of money from scams, shutting down fraudsters' attempts to shift money using cutting-edge defences developed by specialists from across the bank.
    - The team has frozen £18.5m so far and returned £4m to victims.
    - As part of this industry-leading pilot, the team developed a number of new techniques to rapidly analyse data, spotting tell-tale signs, patterns and behaviour to halt fraudsters in their tracks. For all of the frozen funds, we are contacting the sending banks in order to help them get the money back to victims.
- We are a leading supporter of **Take Five** (led by UK Finance) – a campaign urging people to stop and think before giving out their personal details and making transactions.
- We support the industry-wide voluntary code on APP scams to help protect victims of fraud. Our priority is keeping customers' money safe from scams by stopping fraud from happening in the first place. We will ensure that our customers who have done the right thing and followed the best practice in the new code will always be refunded.

ENDS

Note to editors:

UK Finance definition of police/bank impersonation: the criminal contacts the victim purporting to be from either the police or the victim's bank and convinces the victim to make a payment to an account they control.

*July 2019 Lloyds Banking Group

**UK Finance

(Lloyds Bank and YouGov research: Estimated UK adult population was 52,403,344 in 2018 according to the ONS. Further information can be found **here**. YouGov fielded a quantitative survey to a nationally representative sample of the UK population, interviewing 2,018 UK panelists who agreed to take part in research in March 2019.)

MEDIA CONTACTS

Kimberley Hamilton **kimberley.hamilton@lloydsbanking.com** 07557 257 298
Gregor Low **gregor.low@lloydsbanking.com** 07500 078 879