Impersonation scams almost double in first half of 2020 as criminals exploit Covid-19 to target victims

- **Almost 15,000** impersonation scam cases reported in the first half of 2020, **up 84 per cent** compared to the same period last year
- **£58 million** lost to impersonation scams in January to June 2020, **up three per cent** on the previous year
- Public urged to beware of **criminals exploiting Covid-19** to impersonate the police, banks, or government organisations

UK Finance is urging people to be aware of criminals exploiting Covid-19 to target their victims, after figures revealed a sharp rise in impersonation scams in the first half of this year.

Impersonation scams occur when the victim is convinced to make a payment to a criminal claiming to be from a trusted organisation. This could include the police, a bank, a utility company, or a government department.

There were almost 15,000 impersonation scam cases reported by UK Finance members between January and June 2020, an increase of 84 per cent compared to the same period last year. Among these, over 8,220 cases involved criminals impersonating the police or a bank, a year-on-year rise of 94 per cent. Another 6,730 cases involved fraudsters imitating other trusted organisations such as a utility company, communications service provider or government department, an increase of 74 per cent.

£58 million was lost to impersonation scams in January to June 2020, up three per cent on the previous year. This was split between £36.7m lost to bank and police impersonation scams and £21.2 million lost to scams impersonating other trusted organisations.

Scams involving the criminal impersonating a bank or the police often begin with a phone call or text message claiming there has been fraud on the victim's account. The customer is then convinced that to protect their money they must transfer it to a 'safe account' which actually belongs to the fraudster. Other common scams involve text messages or emails claiming a victim must settle a fine, pay overdue tax or return a refund that was given by mistake.

Intelligence reported to UK Finance suggests that the rise in impersonation scams is being partly driven by criminals exploiting Covid-19. These scams include fraudsters sending emails or text messages pretending to be from government departments and offering grants related to Covid-19.

Criminals may also get in touch claiming to be from an airline or travel agency, offering refunds for flights or holidays that have been cancelled due to the pandemic. Additionally, criminals are exploiting the growing numbers of people working remotely, by posing as IT departments or software providers and claiming that payments are needed to fix problems with people's internet connection or broadband or asking for remote access to the victim's computer.

Criminals will tend to research their targets first, using information gathered from other scams, social media and data breaches in order to make their approach sound genuine. They will also often try to rush or panic their potential victims into making a payment, for example by claiming their money is at risk or their account will be blocked unless they act.

Katy Worobec, Managing Director of Economic Crime at UK Finance, commented:

"Criminal gangs are ruthlessly exploiting this pandemic to commit fraud, so it's vital we all work together to beat them.

"We are urging the public to remain vigilant against these vile scams and remember that criminals are experts at impersonating people, organisations and the police. Fraudsters will spend hours researching their victims, but they only need you to let your guard down for a minute.

"Always take a moment to stop and think if you receive a request to make a payment from someone claiming to be from an organisation you trust. Instead, contact the company or organisation directly using a known email or phone number, like the one on their official website."

The banking and finance industry has put in place a range of measures to combat impersonation scams.[1] This includes the Banking Protocol, a scheme that allows bank branch staff to alert police to suspected scams and which prevented £19 million of fraud and led to over 100 arrests in the first half of this year. The industry is also working closely with Ofcom to crack down on number spoofing and with the mobile phone industry to block scam text messages including those exploiting the Covid-19 crisis.

UK Finance is also urging the public to follow the advice of the Take Five to Stop Fraud campaign, which offers straight-forward and impartial advice to help people spot scams and protect themselves against fraud. The campaign recently published an animation emphasising how criminals are sophisticated at impersonating trusted organisations. Consumers are urged to:

- **Stop**: Taking a moment to stop and think before parting with your money or information could keep you safe.
- **Challenge**: Could it be fake? It's ok to reject, refuse or ignore any requests. Only criminals will try to rush or panic you.
- **Protect**: Contact your bank immediately if you think you've fallen for a scam and report it to Action Fraud.

Customers can report suspected scam texts to their mobile network provider by forwarding them to 7726, and forward any suspicious emails to report@phishing.gov.uk, the National Cyber Security Centre's (NCSC) suspicious email reporting service.

Top signs that you are being targeted by an impersonation scam include:

- You receive a call, text, email or social media message out of the blue with an urgent request to make a payment or for your personal or financial information.
- You're asked to act immediately, sometimes with the claim that 'your money is at risk' or 'your account will be blocked' if you don't.
- The caller asks you to transfer money to another account for 'safe-keeping'
- The sender's email address is different to that of the genuine sender