Appendix A

We believe the following examples and case studies will help to demonstrate that the controls mechanisms currently in place for various social media and tech firms are insufficient in stopping cases of fraud and increased intervention is needed.

Investment Scam

Customer interested in invested in cryptocurrency following review of influencers on social media platforms. This influencer had a large number of followers (over 100,000), showcasing wealth and lifestyle, posing with designer goods (cars and luxury accommodation).
Influencers advertised they accumulated their wealth via investment in crypto currency and encourages follower to private message them to "get rich quick". The customer contacts influencer initially via social media platform (Instagram) and the influencer moved communication quickly to another platform, Whatsapp.
The customer started investing small amounts, then was requested further investment needed for return, following a further series of payments totalling £50k customer attempted to access their investment portal and influencer withdraws contact, blocking customer on all platforms.
The customer had no warnings/friction from social media platform around investments of this type or the risks of being request to communicate via another messaging platform. Customer contacted their bank to raise a claim.

WhatsApp Scam

Customer received a message on WhatsApp saying 'Hi Mum, dropped phone in sink, it has water damage, this is my new number.' Customer was asked to make a payment for crypto, her daughter had never mentioned any interest in crypto before but the customer did not want to disappoint daughter so sent the payment.
The customer made one payment of £2,100 which was flagged by the Banks transaction monitoring systems, this included a confirmation of payee no match. The customer called her Bank to release the payment and the Bank warned her about WhatsApp impersonation scams, how they work and how to protect herself from such scams
Further communication between the scammer and customer continues where they coached the customer to send the payment without any further checks. The next morning the customer received a message from her daughter`s genuine number and realised she had been scammed.
In this case the bank have attempted a level of friction for the customer but warnings and controls in social media platforms would support strengthening prevention.

Money Mule Recruitment – Gaming

Customer meets 3rd party through gaming website. The 3rd party engages with customer through chat function and offers them fantastic opportunity to earn money fast – showing how easy it is to use social media as a recruitment tool for economic crime/fraud.
Customer is then encouraged to open bank accounts online and receive money into them , customer is allowed to keep 10% of any money sent to him along as he transfers it to a designated account.
The customers bank then start to receive scam reports from victims of APP and it is clear that the money the customer has received is scam funds.
Customers accounts are blocked and assessed to reviewed for proceeds of crime, this leads to customer being loaded to CIFAS/SIRA. This leaves the customer without access to banking.

We have the following colleague examples that an employee of the bank shared:

Purchase Scam - Holiday booking site

Family member booked a holiday on a site. The site's terms said that you could pay through the site, or you might be contacted by the letter with different payment terms. They said that they were not liable if paid outside their platform, but they allowed it to happen. Family member received an email with request to pay and it was a scam email. The property didn't exist, and the platform refused to reimburse her. She was refunded by her bank!

Social Media account takeover – Instagram

My son had his Instagram account taken over at the weekend. The hacker changed his passwords and recovery email addresses, stopping him from resetting anything. He spent the day corresponding with Instagram who kept sending a password reset link, which went to the hacker, and they rest the password again. My son asked Instagram to suspend the account while he resolved it, and they refused. The account was posting investment scam messages, so it was obviously fraudulent. Instagram said they couldn't do anything, and he needed to set up a new account. In the end, one of his school friands re-hacked his account and returned control to him. The fact that a 17year-old can re-hack shows how weak the controls are.