UK Finance – Written evidence (FDF0058)

UK Finance is the collective voice for the banking and finance industry. Representing around 300 firms across the industry, we act to enhance competitiveness, support customers and facilitate innovation.

Following my appearance before your committee on 17 March 2022, I am pleased to submit written evidence to your inquiry. This brief submission summarises UK Finance's views on tackling fraud in the UK, which we believe should focus on a proactive strategy of tackling fraud at source. The Online Safety Bill, and the second Economic Crime Bill, expected to be announced in the 2022 Queen's Speech, provide excellent opportunities to meet this aim.

In terms of the 2006 Fraud Act, we note that since its assent, the fraud landscape has changed significantly – not least with the advent of various social media platforms since the Bill's enactment, which are now used by fraudsters in several ways to target their victims and enable fraudulent activities. Legislation must therefore catch up with these developments, either through an amended Fraud Act, a new Economic Crime Bill or the Online Safety Bill. The recent announcement expanding the scope of the Online Safety Bill to include both user-generated scam content and online scam adverts is promising, but we would like to see two further changes to the Bill, to avoid this type of fraud from inevitably rising:

- **Create a stronger remit for search engines to tackle online scam advertisements**: The legal requirement for search engines to tackle this form of fraud is weaker and less onerous than for social media platforms as they only have a duty to "minimise the risk" – we propose a more proactive approach for search engines to prevent fraud via scam advertisements by certifying them as 'category 1 firms'.
- **Bring all online advertising providers into the scope of the Bill**: Smaller firms designated by the Government as 'category 2B firms', which host adverts, have not been included. This misses an opportunity to tackle online fraud at all levels and creates a risk that scammers will target these websites.

Furthermore, powers should be introduced that enable public and private sectors and infrastructure (e.g. sharing of Faster Payments System data with Action Fraud) to conduct near real time data sharing in order to prevent fraud. Crucially, these powers must also expand information sharing beyond the financial sector to include law enforcement, TelCos, ISPs and social media. By not including these sectors, a golden opportunity to enhance the data picture to support proactive interventions would be missed.

On suspicious payments, a risk-based approach would be pivotal. To achieve this, banks require the powers to pause and delay suspicious payments for the purpose of an investigation (beyond 24 hours). Legal and regulatory frameworks must also be developed to eradicate the risk that banks currently undertake when returning monies to fraud victims in other banks, so that customers can be reassured that under the right circumstances their money will be returned.

Lastly, we recommend enhancing powers to address the withdrawal and cashing out of funds obtained through Authorised Push Payment (APP) scams. The collective agreement between industry, HMG and regulators toughens the stance on Money Mules, Money Service Bureaux and Crypto exchanges, up to and including the ability to refuse payments, but more can be done. Technology like the Money Insights Tactical Solution (MITS) has been developed to trace and freeze stolen money, however, no legal framework to support this approach exists. It is the industry's view that the ability to move faster than the fraudsters is contingent on the development of such a framework.

22 April 2022