techUK – Written evidence (FDF0059)

Introduction

The nature of economic crime is changing in response to the digitisation of the global economy. As we have all moved our lives online and increased our digital footprint, fraudsters have found ways to adapt their sophisticated techniques to prey on the vulnerabilities of society. The pandemic has accelerated this change and the pace of change will further accelerate as criminals and bad actors become more technically adept and better resourced.

The UK is at the heart of digitising economies which has a positive impact on growth and skills for society and businesses alike. However, this also means we are experiencing rapid innovation in economic crime with new forms of technology for criminals to exploit. Tech companies experience part of a fraudster's journey with a range of other private sectors also having their systems exploited by criminals. The fraudster takes victims on a journey through various services - including ISPs, tech platforms, insurance, and financial – and the types of fraud may differ depending on the victims' vulnerabilities and functionalities of services.

Overall, individual companies and services have systems in place to combat illegal activity but to beat the criminals more needs to be done to support better law enforcement responses and enable cross-sector collaboration. techUK was delighted to give oral evidence to the Committee to outline the need for a whole system change response to combat fraud. This written submission aims to outline at a high level how the tech sector is currently responding to the threat of fraud while providing some insight into the ongoing challenges and concluding with a proposed recommendation for the Committee to consider as part of its Inquiry.

Tech sector response to fraud

Across techUK's membership, many different companies are acting against fraudsters. techUK has around 250-300 members working across the cyber domain, many of which are providing the technological capability which underpins and enables people to work and live online.

Telecom operators and Ofcom are working together to crack down on nuisance and fraudulent phone calls and SMS text messaging, which has grown over the course of the pandemic. Digital identity verification systems are helping reduce fraud by using cutting edge biometric technology, while offering enhanced levels of privacy and security to improve the protection of customer data against cyber threats.

Advertising intermediaries and social media platforms continue to work with the Advertising Standards Authority on the scam ad alert scheme, with recent developments including partnership with the National Cyber Security Centre to help support the government's takedown notice.

techUK's larger platform members have been collaborating with the banks and law enforcement through the Online Fraud Steering Group[1] with achievements including a pledge of 1$ ad credit support to Take 5 to Stop Fraud and the

[1] OFSG is a public/private group focused on reducing the threat from fraud in the UK. The formation of the OFSG which is co-chaired by the NECC, UKF and techUK, follows on from a roundtable hosted by Gov Ministers in April 2021.

commitment to introduce a new advertising onboarding process that requires UK regulated financial services advertisers to be authorised by FCA prior to serving financial services adverts on their sites.

Challenges to combatting fraud

techUK has been exploring how fraud is dealt with across government. It appears that this activity is on the fringes of government departments and regulators who understandably all have a specialist area of interest. However, due to the nature of fraud being led by patterns of behaviour, techUK believes that a fragmented response to this issue will not be effective in solving the problem in the long term.

One of the biggest challenges for collaboration is that there is no commonly understood definition of 'fraud' or 'online fraud' - these terms mean different things to different organisations - depending on where they sit in the ecosystem. For example, while a bank experiences the cashing out of fraud, a tech company may experience activity that could be fraudulent and will likely only have certainty that this activity is fraudulent after the cashing out has taken place. To understand how and when to act at any point in the value chain you need to understand what is happening at other points in that value chain. Criminals actively seek to exploit the gaps between the silos. To beat the criminals, we need a digitised whole system response involving public and private sectors.

Furthermore, digital technologies have 'distinctive features which make digital businesses and applications unique and innovative',[2] with no one tech company or platform being the same. Given this distinction across the sector, any one size fits all solutions to combatting fraud may not be proportionate to address different levels of risk of fraud types. techUK supports the Treasury Select Committee sentiment that there is no 'silver bullet' to combatting fraud[3] and instead different public and private sectors need to operate and work with each other to identify shared challenges and form collaborative solutions to mitigate fraud.

techUK key recommendation

techUK would like to see the Committee consider how the solution requires a whole system change response. Ultimately, a range of different sectors, organisations and society are vulnerable to sophisticated criminals, and we should not seek to engage in blaming different sectors but instead on building relationships, building trust, and forming collaborative cross-sector solutions.

22 April 2022

[2] DCMS Plan for Digital Regulation, 2021

[3] Treasury Select Committee Report on Economic Crime, 2022