New Legislation Needed to Fight Cyber Crime

Robert Brooker is Head of Fraud & Forensics at PKF GM, Chairman of the London Fraud Forum and nationally recognised expert in Fraud prevention. Robert explains why he believes the Fraud Act of 2006 rapidly needs updating to challenge todays Cyber Crime threat.

Action Fraud saw a reported £9.6million lost by victims of cyber crime in 2020/21 and the UK economy is reported to have lost £2.5billion to fraud and cyber crime in 2021. Increasingly more activity occurs online, and this is a growing trend, so why is fraud so prevalent, and what are the Government doing about it and what can we all do to help, if anything?

Technological progress, including the move to additional online business models following the Pandemic, means that many UK businesses now work as hybrids; online and remotely. They may also have international operations supported from offshore hubs. Eventually, advances in the metaverse will have an impact on how fraudsters perform, however it is too fresh to understand the impact of this yet.

One of the key ways that technology can mitigate these developing risks, is by humanising and encouraging how to keep personal details safe in a digital world. An absence of understanding or awareness exposes individuals to online fraud, victims often have their personal details or money taken because of online fraud and receive little assistance from law enforcement. This is often because the fraudsters are based outside of the UK, making practical and effective law enforcement action difficult.

Technology and the appreciation of online activity enables global fraudsters to be able to access the UK public with little chance of punishment, and this is only likely to upsurge in future as technology becomes implanted as a way of life.

The obstacles to tackling global fraud are numerous, the most impacting being the complexity of cyber crime. The online fraud that we see often includes a multitude of websites and platforms connected, often based overseas, with various methods of communication used and international groups involved.

Additionally, the use of offshore bank accounts ensuring the money leaves the UK immediately the fraudsters receive it, making it difficult to recover. The speed at which technology is developing only adds to this complexity, and fraudsters can continue with these trends quicker than law enforcement can trace them.

Consumers today are much better informed around the risks of fraud than ten years ago, but although individuals receive and recognise the big messages around fraud risks and what to look out for, it is not the first thing that they think about. Whilst awareness is greater than ever before, when pressure is applied, individuals do not recognise fraud still, until often it is too late. There continues to be a lack of consistency on where to go for advice or how to report a fraud.

"One of the key ways that technology can mitigate these developing risks, is by humanising and encouraging how to keep personal details safe in a digital world"

Unfortunately, a long-standing perception that fraud is a victimless crime, certainly when it is committed against a business does not help. Whilst this is changing as the issue grows and more individuals are impacted, this perception leads to a less favourable experience for fraud victims, across both public and private sector, as well as within the general neighbourhood.

Fraud is not a victimless crime and the impact is severe in terms of financial loss, the cost of the investigation, replacing staff if an insider fraud, the loss of goods, the reputational damage to a business and subsequent, loss of confidence to the proprietors. All are unseen to the outside world.

The Fraud Act was an excellent and necessary requirement, when introduced in 2006 as specific legislation defining Fraud and its remedies were greatly needed. It has allowed law enforcement to treat fraud as a criminal offence and the public to recognise fraud.

Unfortunately, due to the ever-changing nature of fraud, we believe the Act at 15 years old, is now outdated, because it does not reflect the issue and complexities of digital fraud or recognise the impact of the Insider Threat. Coupled with the maximum sentence only being 10 years and the value of fraud dramatically increasing, this seems a little inadequate for £10/20M worth of fraud.

There needs to be legislation which covers the online space and digital fraud – the Online Safety Bill will likely address some of these areas, but digital fraud will need to be defined in legislation. A legislative remedy to encourage the private sector to be more engaged with combatting fraud could be to include a Failure to Prevent section, similar to section 7 of the Bribery Act 2010.

Additionally, the newly introduced Economic Crime Bill will aim to tackle economic crime, including fraud and money laundering, by providing greater protections for consumers and businesses. David Postings, Chief Executive of industry body UK Finance, welcomed the provisions made in the Bill to tackle fraud and scams, which he described as the "most prevalent type of crime" in the country. "This Bill should focus on measures that prevent fraud happening in the first place and provide greater enforcement powers to tackle those who commit economic crime,"

Fraud continues to breed at a rapid pace with no signs of letting up anytime soon. The fraudsters recognise the weaknesses in recognising victims. The Fraud Act at 15 years old, is now outdated, does not reflect the complexities of digital fraud, or recognise the impact of the Insider Threat. The Online Safety Bill may address some of the voids, but until such time, as legislation may act as a deterrent, fraud will continue to be the crime of choice.

About the author:
Robert Brooker

Head of Forensics and Fraud PKF GM, Robert has worked in private and public sectors within financial crime for over 20 years. He is also Chair of the London Fraud Forum, (NFP) bringing public/private sectors together to fight fraud, bribery and corruption.

Scan the QR Code