Report on Resilience First Webinar

12 November 2020

'Economic crime in a Covid-19 world'

Speakers:

Graeme Biggar CBE, DG National Economic Crime Centre, National Crime Agency

Chris Greany FCMI, Managing Director, Templar Executives Ltd

Paul Davies, Head of Loss Prevention & Security, Selfridges

Chair:

Nicola O'Connor, Legal Director, Bird and Bird

Key Messages

- Fraud and financial crime remain the largest crime type in the UK and therefore require an effective counter-prevention and detection strategy. Fraud makes up about 35% of reported crime but reported crime is believed to be well below the actual level of illegal activity.

- Covid-19 pandemic has created new opportunities – 'a perfect storm' – for economic crime. The first weeks of the pandemic (lockdown) saw reported fraud drop by about 25% but, sadly, it quickly returned to previous fraud levels and the trend of growth

- The type of frauds did change. A number of specific Covid frauds targeted against individuals emerged, including involving fake PPE and test kits, albeit they only ever represented 2-3% of the total reports received by Action Fraud. There was also significant growth in online shopping fraud – matching the growth in online shopping, as well as increases in investment fraud and romance fraud – two high-harm, high-value types of fraud. And there was new opportunity to fraudulently target the schemes that the government introduced to help support businesses and individuals.

- The increase in fraud has thrown into sharp relief the lack of resource for fraud investigations in the UK and prompted calls for organisational reform. Fraud attracts less than 1% of policing. The response to fraud by many forces has been 'completely forgotten'. It is perhaps unreasonable to ask one police force (CoLP) to act as a national anti-fraud agency with no legal remit to task other forces.

- According to one speaker, tackling fraud needs a much better prevention and detection strategy. It requires a national fraud strategy that prevents rather than detects economic crime, a single governance and leadership, and a more intelligence-led approach. Using intelligence, it should be possible to design out fraud and target the investigative resources against groups that are seen to be driving the most severe forms of harm rather than trying to investigate every single report.

- It is necessary to move away from the idea that prosecution is the answer to the problem. Businesses do have to protect themselves and their customers and some have to spend more money on their staff training to protect their business.

- For retail, trading remains tough, with customer footfall down in all major cities. Stores have limitations in capacity to comply with social distancing while operating costs remain high in comparison. As a risk management function, stores have had to be more agile in the approach to crime as the focus of commercial operation has changed from being physical to digital.

- In initial responses to Covid, it has been necessary to be more reactive and responsive than proactive. For instance, when stores were closed in lockdown, efforts were focused on digital fraud, third-party or carrier-logistics theft, and customer-return fraud. When stores reopened, there was a significant increase in cash transactions which were both unexpected and exceptional. Focus then turned back to the risk of money laundering or counter cash and other crimes at the point of sale.

Note: As simple poll of participants to the question: 'Have you or your company been a victim of fraud or cyber-crime since March?' revealed a Yes for 11% and a No for 88%.

A copy of the full video recording of the presentations, and the subsequent discussion, can be found here.

Speakers' Biographies

Nicola O'Connor

I have spent my career defending individuals and organisations charged with serious fraud and white-collar offences. I recognise the daunting prospect of being involved in the criminal justice system for the first time and having to consider additional reputational and professional issues during the process.

Over the years, I have advised individuals and organisations under investigation or facing prosecution by a variety of agencies such as HMRC, National Crime Agency, Serious Fraud Office and Crown Prosecution Service. I regularly advise clients facing confiscation proceedings and restraint orders under the Proceeds of Crime Act.

Graeme Biggar CBE

Graeme was appointed Director General, National Economic Crime Centre (NECC) in March 2019.

The NECC is a collaborative, multi-agency centre established to deliver a step change in the response to tackling Serious Organised Economic Crime. It has been set up to protect the public, prosperity and UK's reputation by leaving no safe space for criminals and reducing the threat of Economic Crime.

Graeme joined the agency from the Home Office where he had been Director National Security since 2016, providing leadership on the pursue element of the counter terrorism strategy and hostile state activity. His experience includes helping shape the response to the 2017 terrorist attacks, and the Salisbury attack, and overseeing the Investigatory Powers Act implementation programme across government.

Before joining the Home Office, Graeme worked for the MoD, in a series of policy and change management positions. He was Chief of Staff to the Defence Secretary from 2013 until 2016.

Chris Greany FCMI

An accomplished speaker, media commentator and thought leader, Chris has international experience advising executive boards, governments and regulatory authorities. At Templar, he oversees the core delivery of cyber and information security engagement and change programmes across an international customer base including blue chip, public sector and SME clients.

He is a member of the Cyber Security Advisory Board for the Institute of Asset Management, founding partner of the Global Cyber Alliance and a former member of the Bank of England's Cyber Security Board. Widely published, his latest work on insider threats, 'Managing Cyber Security Risk 3', is written with Jonathan Reuvid Books (2019).

Previously, as Managing Director at Barclays he implemented global security capabilities including investigations, cyber forensics, data protection controls, the group insider-threat programme, and the build of security operations centres across three continents.

Paul Davies

Paul Davies is Head of Loss Prevention & Security for Selfridges, where he leads a large and diverse function that has been created over the past three years, with specialist teams for Investigations, Financial Crime, Retail and Supply Chain Loss Prevention and Security. He is also responsible for Selfridges Business Resilience planning from business continuity to crisis management and recovery.

Before joining Selfridges, Paul spent three years working as an independent consultant / project manager where he partnered with a variety of retail, logistics and hospitality clients on broad range of security and risk management projects.

Over the last 17 years, Paul has held a variety of risk management and security roles, in companies such as Dixons Retail, Asda and Amazon where he also led the function in the UK.