

# **Public Private Threat Update**

## **Economic Crime**

## **Key Judgements**

**July 2019**

## Background

In January 2019 the Economic Crime Strategic Board (ECSB) commissioned a joint public/private sector threat update (PPTU) of the key economic crime threats facing the UK in order to inform the UK's Economic Crime Plan. The update looked at the combined latest public/private understanding of money laundering, fraud against individuals and businesses, and international bribery.

## Key Judgements

### Fraud

- Reported fraud in the UK continues to increase in both number of reports and total volume with GBP 2.2 billion of loss reported for the financial year 2018/19. This represents a 38.1% increase in loss when compared to the previous year and a 9% increase in the number of fraud crimes reported. Other indicators of fraud have also increased the crime survey of England and Wales (CSEW) estimated there were 3.6 million incidents of fraud during 2018, an increase of 12% from the previous year.
- 86% of reported fraud is now estimated to be cyber-enabled. Technological change has presented new opportunities for fraudsters who can relatively easily spoof their true identity and location, making them more difficult to apprehend. Victims include organisations and individuals of all ages.
- The volume of personal data available online is making social engineering type scams more prevalent and sophisticated. Social media platforms are also being used to identify potential victims.
- Businesses remain vulnerable to exploitation from the insider threat, where employees are either used by criminals for a variety of fraud-related tasks or conduct the fraud themselves.
- Criminals engaged in high level organised fraud regularly use the services of individuals with accountancy and legal skills as well as other professions. They can be used either wittingly or unwittingly, and can add legitimacy to fraudulent approaches.
- Abuse of identity remains a key enabler for fraud. Modern printing techniques mean that forged documents are increasingly difficult to spot and impersonation is also commonly used when applying for financial services.

### International Bribery

- Some UK registered companies pay bribes overseas in order to obtain or conduct business. Sectors most likely to be at risk are those where public officials have a high level of involvement e.g. the extractives industry, or where there are only a few companies operating in the sector, such as in aviation.

- Whilst bribe payments are still being paid through intermediaries to companies in secrecy jurisdictions, other forms of bribes such as the payment of school fees, are increasingly being seen.
- It is a realistic possibility that the UK's exit from the EU will impact the prevalence of bribery and corruption over the next five years, as UK companies potentially come into greater contact with corrupt markets.
- Whilst technological developments and adaptations may help reduce countries' levels of corruption, the public and private sectors will have to remain vigilant to the fact that such solutions may lead criminals to developing alternative, more complex methods to pay bribes.

### Money Laundering

- The UK's financial sector is a global centre for legitimate business. It is also attractive to money launderers because of the range of professional services on offer, as well as the complex and varied ways it offers to launder money.
- There is no accurate estimate of the total value of laundered funds impacting on the UK. Yet given the volume of financial transactions transiting the country, it remains a realistic possibility that the scale of money laundering impacting the UK is in the hundreds of billions of pounds annually.
- Criminals abuse UK and offshore corporate structures to launder and conceal their illicit finance. Trust and Company Service Providers (TCSPs), some of which are based overseas, are used to set-up many of these structures.
- The use of money mule accounts to launder the proceeds of crime remains a key threat. Social media platforms are increasingly being used by criminals to recruit money mules, with students and school age children being drawn into this activity.
- The criminal exploitation of those with accounting and legal skills poses a significant money laundering threat.
- The majority of Trade based money laundering (TBML) schemes identified involve open account trading where payments for goods and services are received from numerous third parties.
- Criminally-engaged money service businesses (MSBs) are continually adapting and evolving their methods of operation in order to avoid detection.
- Criminals, as early adopters of new methodologies, are attracted to financial technologies, Payment Service Providers (PSPs), challenger banks and cryptoassets. This diversification provides criminals with more opportunities to place and layer illicit proceeds.

## **Why this work matters?**

1. This is the first time that a joint economic crime threat update has been produced involving a broad range of private sector organisations. Whilst previous NCA assessments have drawn on a range of data, including that provided by the private sector, this is the first time a joint threat update has been written.
2. The PPTU has directly shaped the UK's Economic Crime Plan 2019-2022, which has been developed by HMT, the Home Office and UK Finance. This plan will shape the UK's response to economic crime for the next three years. Law enforcement and the private sector are keen to work together on further updates as well as commissioning "deep dive" assessments into collective knowledge gaps that have been identified.
3. The PPTU clearly demonstrates the value in bringing together a wider range of partners to help inform an understanding of the threat. For example, it confirms that the public and private sectors broadly agree with the main areas of concern and intelligence gaps.
4. The strong working relationships established across all levels of the public and private sectors provides an excellent foundation for future joint assessments.