City of London Police – Written evidence (FDF0031)

Introduction

1. The City of London Police is the National Police Chiefs' Council Lead for Economic and Cyber Crime and National Lead Force for Fraud. The City of London Police operates Action Fraud and the National Fraud Intelligence Bureau, funded by the Home Office, which is the national reporting and recording centre for fraud and cyber crime. It also provides training and continuous professional development for the police and private sector workforce through its Economic Crime Academy.

2. Along with the National Crime Agency, Serious Fraud Office and the Crown Prosecution Service, the City Police is part of the National Economic Crime Centre which leads the cross-system law enforcement response to fraud.

3. The City Police and the City of London Corporation as police authority (acting through its Police Authority Board), have a unique role to play in the fraud landscape, providing a bridge for law enforcement into financial institutions and, importantly, also into the fintech sector. With the support of the City Corporation and stakeholder groups such as UK Finance, the City Police has consistently shown how it can harness and work with the private sector in the pursuit and prevention of the perpetrators of fraud.

Fraud Landscape

Threats

4. Action Fraud records fraud and cyber crime reported by the public (individuals) and the private sector. It also receives reports through UK Finance and Cifas. Reporting has increased by around 10% year on year and we predict this trend will continue. However, based on the Crime Survey of England & Wales data, fraud is under reported to the police by an estimated 85%. Based on Action Fraud data from 2020/21, the crime types that present persistent threats to the UK public and businesses are:

    - Courier fraud
    - Cheque and bank account fraud
    - Dating/romance fraud
    - Investment fraud
    - Payment diversion fraud

5. These crime-types cause harm to individuals or businesses and have both a psychological and financial impact. These fraud types continue to be some of the highest volume categories of reported fraud and losses and are reported nearly every week in the year.

6. Other key threats to the UK include online shopping and auction fraud which is still a commonly reported offence and has increased in both volume and loss amounts over the last year.

7. It is estimated that over 80% of fraud is enabled through online technology. This includes 16% of crimes through social media platforms. Unlike other crime, fraud rose during the pandemic lockdowns. This was primarily due to increased adoption of online activities such as shopping

and dating. Increased online socialising will lead to more opportunities for fraud offenders to target UK victims from all over the world. The growth in romance fraud during the pandemic illustrated how a greater reliance on online social platforms can expose users' vulnerability. Measures in the Online Safety Bill will help to mitigate this.

8. Telecommunications continue to be an enabler for fraud with the use of prepaid and unregistered mobile phone SIM cards used by criminals and mass phishing through SMS/text messaging used to target the public. Greater regulation in this sector would help to mitigate this.

9. Fraudsters often pose as trusted and recognised entities, such as government bodies, solicitors, law enforcement, utilities suppliers, tradespeople, and financial services professionals, to engage their victims. Increased use of internet services and fewer face to face transactions means that corporate identities can be cloned or faked. This will require greater reliance on multi-factor authentication and methods for verification and assurance of digital identities.

10. Technological advances such as 'deep fake' imagery will feature in methodologies targeting UK victims via messaging, video calls or online dating sites. This can be mitigated by online platforms planning for this and putting barriers in place to recognise this technology and prevent its use.

11. The continued use of 'money mule networks'[1] to receive, move and conceal the proceeds of fraud is an ongoing and persistent threat evidenced across many fraud types and continues to facilitate the movement of fraudulent funds as well as access to victims across domestic and international jurisdictions. The recruitment of money mules for use in fraud has continued over the past year on both digital messaging services and social media platforms.

12. During times of economic uncertainty there is often an increase in fraud as people seek to improve their financial situation. With the cost of living crisis resulting in greater levels of economic hardship, there may be increased recruitment of money mules and increased vulnerability to investment fraud, advance fee loan schemes, and online shopping fraud where less disposable income leads to more risk taking to find cheaper alternatives.

<u>International</u>

13. The City of London Police estimates that nearly half of fraud has international links. This includes criminal networks that operate within both the UK and internationally and considers both offender location and international money flows.

14. Levels of cooperation in terms of intelligence sharing and joint investigations are variable depending upon the jurisdiction. The City of London Police has developed partnerships with law enforcement agencies to overcome this. This includes having economic crime officers seconded to the New York District Attorney's Office and Interpol who build international relationships and facilitate intelligence sharing and joint operational activity.

---

[1] A money mule is a person who receives money from a third party in their bank account and transfers it to another one or takes it out in cash and gives it to someone else, obtaining a commission for it.

15. Action Fraud crime reports are routinely monitored to identify overseas links and opportunities to work with overseas law enforcement to address fraud threats affecting the UK. For example, a recent initiative to tackle romance fraud involved targeting criminals overseas committing fraud against UK citizens. A partnership between the City Police, the National Crime Agency and law enforcement in Ghana was developed so policing could send intelligence referrals to the Ghanaian authorities where they had identified suspects based in Ghana, or with a link to the country. This has led to over £175,000 being repatriated to UK victims of romance fraud. There are 10 active investigations in Ghana into suspects believed to be defrauding victims in the UK as a result of these referrals (with further planned) and have been 4 arrests to date. In December 2021 there was coordinated operational activity between the UK and Ghana to disrupt a money mule network linked to multiple Ghanaian romance frauds.

16. Another example of law enforcement partnerships relates to computer software service fraud being perpetrated by companies operating in India. The City Police worked with Microsoft to develop the intelligence and supported Indian authorities to take enforcement action by providing vital witness statements detailing the victims' dealings with the companies concerned. This resulted in 88 arrests and action taken against 47 call centres.

Prioritisation

17. Fraud is not always treated as a priority. Companies and government regularly make trade-offs between security and ease of customer journey/doing business. The speed of banking payments is an example.

18. Fraud competes with numerous policing priorities including those that cause significant physical harm to the public such as violence and sexual exploitation. At a national law enforcement level, it also prioritised below other serious and organised crime threats such as drugs.

19. Policing operates a model which applies resources based on threat, harm and risk which means vulnerable victims of fraud are prioritised. Making fraud a Strategic Policing Requirement and including it within the National Policing Board performance measures alongside crimes such as burglary would improve prioritisation, as would inclusion of fraud within all local Police and Crime Plans which are developed by Police and Crime Commissioners.

Action to Tackle Fraud

Structures

20. Fraud is a high-volume offence and the response requires partners and communities at local and national levels to work together systematically in order to address the threat collectively. Policing is part of a wider law enforcement system responsible for tackling fraud. The National Economic Crime Centre (NECC) provides leadership and coordination of the national law enforcement response. The National Crime Agency (NCA) and Serious Fraud Office (SFO) are responsible for serious and organised fraud above the capability of policing. Trading Standards is a key partner at a local level. The Cabinet Office's Government Counter-Fraud Profession has responsibility for fraud against the public sector.

21. Currently approximately 90% of investigations into fraud against the individual and private sector are undertaken by policing. Fraud spans different levels of criminality from serious and organised to opportunistic. Fraud is cross border and police capabilities are required to respond to the large volume of fraud cases spanning multiple force areas that are not cross-agency. These cases often have a high cumulative value due to the volume of victims and require specific expertise but fall below the serious and complex threshold of the NCA and SFO.

22. The National Fraud Policing Strategy includes a roles and responsibilities grid which details expected capabilities at a local, regional and national level. However, these capabilities are inconsistent across forces at this time. The use of local resources in fraud are most effectively targeted towards victim care, protect and investigation into local fraud offenders. Regional resources are most effectively targeted at organised crime groups involved in a wide range of criminality that operate regionally. These teams need to operate as a national network and be able to draw upon specialist expertise and national capabilities such as intelligence, forensic accountancy and overseas financial enquiries.

23. A national police capability is also required for investigations that are too large or multi-jurisdictional for regional capabilities but below the threshold of the NCA and SFO. This is currently provided by the City of London Police as the National Lead Force for Fraud.

24. The City of London Police was appointed the National Lead Force[2] for Fraud, following the Attorney General's Review of Fraud in 2006. The headline recommendations of the review were the precursor to the force's current responsibilities which include:

    - setting the national fraud policing strategy
    - leading and coordinating the police's 4P response to fraud
    - national fraud and cyber crime reporting and recording (Action Fraud)
    - triage, analysis and allocation of crime reports to policing and other law enforcement for protect, pursue and intelligence (National Fraud Intelligence Bureau)
    - advisory support for forces investigating complex fraud (National Fraud Operations)
    - investigation of nationally significant, serious and complex fraud (National Fraud Operations)
    - workforce development, including training, continuous professional development and dissemination of good practice across police forces (Economic and Cyber Crime Academy)

25. Central reporting is essential to provide a consistent service to victims nationally and to ensure high standards of crime recording. Central reporting is also necessary to enable early identification of trends required for effective investigative interventions and timely protect advice to the public (the most cost effective and harm minimising intervention available).

---

[2] HMICFRS has endorsed the national lead force model stating that activity by a national lead force to encourage the adoption of effective practices and techniques by forces is necessary to improve the police response.

An estimated 78% of frauds involve offences where suspects and victims do not live in the same force jurisdiction.

26. Action Fraud provides efficient processes for recording crime. It has a 98% utilisation rate by call handlers (compared with 57% in police control rooms) and higher than average digital contact for policing. Victims can report crime at first point of contact to trained call handlers who collect all information needed to commence investigations, assess vulnerability and provide victim support. This compares to 101 where there are often two points of contact required in order to record a report. Without Action Fraud about a million additional contacts would be made to police 999/101 centres per year and about 600,000 reports would have to be recorded. This is at a time when HM Inspectorate of Constabulary and Fire & Rescue Services (HMICFRS) is reporting that police control rooms are in danger of being overwhelmed by demand. Analysis of how the process would be delivered locally has indicated it would result in a fourfold increase in costs / resources. Prior to the establishment of Action Fraud, the service to victims trying to report was unreliable due to a lack of fraud expertise within force control rooms and front counter staff. Victims were often advised that fraud was a civil matter. Action Fraud provides assured reporting procedures by trained call handlers that encourages fraud reporting.

27. Steps are being taken to improve call answering times and reduce the time callers spend waiting in queues. These improvements respond to recommendations made in a review of lead force functions led by Sir Craig Mackey QPM. This includes exploiting new technologies through the introduction of a chatbot to provide a better user experience and to free up call handlers to support more vulnerable victims, and improvements to the web reporting service.

28. Action Fraud's Economic Crime Victim Care Unit assesses the needs of approximately 80,000 victims a year providing a service to victims of fraud and cyber crime whose crimes are not investigated. Victims receive a focused and targeted service providing a national standard of care and support, by working with forces and safeguarding partners at a local level. In the last year, only 24 service users have become repeat victims and direct interventions have resulted in prevention of an estimated £700,000 in victim losses. Since January 2021, the unit has helped victims to secure reimbursement for £2.2m in losses.

29. The National Fraud Intelligence Bureau (NFIB) reduces manual processing of crime and information reports through a central analytics system that automates triaging and linking of crimes in seconds. It provides a central crime review service with access to national data sources that saves police forces time by developing lines of enquiry on their behalf more efficiently than could be achieved locally. It is estimated this saves forces approximately 400,000 hours per annum. It links crimes from across the country preventing the duplication that would occur if each force was investigating crimes based on local victim reports. This increases the likelihood of investigation due to the true scale of offending being identified which would not be apparent from local data. Without the NFIB's analytical capabilities, series of linked offences would not be identified. Inevitably, this would mean individual forces would investigate crimes committed by

the same person without the benefit of knowing the suspect was of interest to another force. This would lead to multiple, unstructured enquiries being made by different forces to the detriment of a prosecution case often through difficulty in disclosure processes.

30. The City of London Police is in the process of procuring a next generation fraud and cyber crime reporting and analysis service. Working with law enforcement, government agencies and the private sector, the transformation programme strives to create an accessible service for all to report fraud and cyber crime. It will use new and enhanced technology and data analysis to disrupt organised crime, help protect businesses and the public from deception and bring more criminals to justice. The aim of the programme is to redesign how fraud and cyber crime offences are reported by the public and organisations, and to streamline the review process of these reports. It will continue to be reliant on policing and the wider law enforcement system to investigate its crime and intelligence packages.

31. In 2020, the City of London Police established a Lead Force Operations Room. This is the mechanism through which it coordinates operational activity and provides peer support to investigators across the country. It connects directly with regional and national tasking forums to dial up the whole system in line with emerging threats, from tactically referred cases through to nationally coordinated campaigns tackling high harm fraud typologies such as romance, courier, investment and payment diversion fraud.

32. Working with the City of London Police Authority, the City of London Police has an engagement programme to encourage greater understanding and prioritisation of fraud threats across policing. The programme includes working with the Association of Police and Crime Commissioner to improve performance reporting, so Police and Crime Commissioners are better able to hold their forces to account for their fraud response. During 2022, the City of London Police will be visiting all forces and regions to identify good practice and provide support and guidance. The programme will help forces to identify opportunities to improve their fraud response and build on the findings of HMICFRS reviews.

33. A substantial part of the UK's capacity to investigate fraud is invested in the City of London Police specialist teams funded by the Home Office, the City of London Corporation and the finance and insurance sectors. Their average caseload sits at over 400 fraud investigations affecting thousands of victims. The City of London Police has developed an innovative approach to managing significant serious and complex fraud investigations working partnership with the Crown Prosecution Service (CPS). This is underpinned by a set of key operating principles focussed on delivering against the most challenging fraud investigations inside a two-year timeframe, while operating within a clearly defined framework of governance and risk oversight. Since the implementation of the new model 81% of its serious and complex fraud investigations were concluded within 2 years with a 100% conviction rate for cases reaching charge. This has been developed as a model of good practice and efficiency and is being shared across policing. Around 25% of this team's caseload comprises investigations for police forces and regions that are beyond their capabilities.

34. The City of London Police's Economic and Cyber Crime Academy is the only police training unit in the UK that delivers specialist fraud training. Its curriculum is linked to the College of Policing Professionalising Investigations Programme, and it holds a national register of fraud investigators from across policing. Its work is crucial to developing and maintaining a workforce with the skills and knowledge required to effectively investigate fraud. It trains around 1,000 people in economic crime investigation a year. It has an online learning programme developed in partnership with the University of Coventry provided free of charge to volume crime investigators.

Resources

35. Funding for Action Fraud and the National Fraud Intelligence Bureau (NFIB) has not kept up with demand. There has been a 41% increase in reports to Action Fraud over the last four years. The police funding formula is out of date and does not take account of fraud demand. This has meant policing has not been able to keep pace with the rapid increase in reported fraud offences. The current review of the police funding formula must incorporate fraud within its demand indicators.

36. The Home Office has secured a £400m uplift in funding for fraud capabilities over the next 3 years through the recent spending review. Approximately £100m will be invested in policing to create a new national network of investigators across the regions in England & Wales and in the City of London Police. This will increase police capacity for high harm fraud investigation including online fraud. The network will be led and coordinated by the City of London Police and a people strategy is being developed to create new pathways into fraud. The funding will also enable the roll out of the Economic Crime Victim Care Service to all police forces to improve consistency of victim support and reduce repeat victimisation.

37. The Fraud Investigation Model developed by the City Police and recognised as Authorised Professional Practice by the College of Policing provides police investigators with a best practice framework for serious and complex fraud investigations. The Economic and Cyber Crime Academy has a range of training courses for counter fraud capabilities including investigation, crime prevention and victim support. It also provides training in online investigation and cryptocurrencies and other emerging issues.

38. The Specialist Fraud Division (SFD) of the CPS would benefit from expansion, particularly with the planned uplift in police resources over the next few years. SFD prosecute the most complex and/or serious economic cases for the CPS.

39. The complexity and size of fraud cases continue to result in delayed and long trials which has been compounded by court availability during the pandemic. Backlogs in the courts system also affect confiscation hearings, which are essential to victims getting their monies back. Currently judges personally decide the extent of video viewing used in their courts, some using it significantly less than others. Remote hearings should become the norm in enforcement, confiscation and other associated proceedings under the Proceeds of Crime Act. This includes restraint proceedings in Part 2 of POCA. This would allow justice to be done more quickly.

40. Although specialist economic crime courts are not currently in existence, the City of London Corporation continues to progress its plan to build the City of London Law Courts, a flagship for Her Majesty's Courts and Tribunal Service and the Ministry of Justice containing dedicated 18 court rooms: Crown, Magistrates, County and Civil Court. The idea of specialist Economic Crime Court sessions nationally staffed by specialist judges and staff would be welcomed, alongside specialist regional courts.

41. A mandatory CPD training module on fraud and its impacts on the victim and their vulnerability, should be introduced for all the judiciary, regardless of specialism. This should form a core element within the Judiciary College digital training and leaning and development offer.

Prevention

42. In the same way organisations are required to ensure their physical products do not cause harm to consumers, there should be an obligation to ensure digital and other services also provide appropriate protections from fraud. The Online Safety Bill is a first step towards this. The City of London Police supports measures that place liability on corporations to prevent fraud. It brings discussions of fraud prevention to an executive level and encourages measures and auditable processes as well as additional controls. An example being in the modern slavery area where companies have to track and prove that they are implementing measures, which has led to greater corporate responsibility and a dedicated prevention response.

43. Through Action Fraud reporting, the City of London Police is able to identify the latest fraud trends and uses this to raise awareness of how the public can protect themselves against the latest threats. This is delivered through a range of channels including social media, traditional media, direct communications / alerts and other intermediaries such as charities and community groups. Its social media campaign about covid-19 vaccine fraud reached over 1.1 million people. A survey of recipients of its alerts showed that as a result 81% of respondents found it easier to identify a fraud and 62% changed their behaviour to better protect themselves.

Legislative Remedies

44. The Fraud Act 2006 simplified the law in relation to fraud. It brought many offences under one banner. Consideration could be given to adding further offences to the current legislation which may suit more complex digital cases/online fraud and make the case easier to prove. Online frauds generally make a misrepresentation at some stage. One example would be to address people using company brand names to push their criminal websites further up internet search results, inciting unsuspecting members of the public to hand over money or personal data to criminals.

45. The Fraud Act does not cover cyber dependent fraud, where computers are key in the commission of the offences. Frauds committed under this category are usually prosecuted under the Computers Misuse Act 1990 which itself is in need of updating. The Criminal Justice Act 1976 is further limited due to its age.

46. Offences such as conspiracy and money laundering, can be used if fraud is too difficult to prove. Policing also uses legislation under the Financial Services and Markets Act as an effective piece of legislation.

Prosecutions

47. There would be benefit in prosecutors and investigators collaborating more at an early stage to align investigative and prosecution strategies, including the approach to disclosure and maximising opportunities for civil recovery/investigation (for proceeds of crime). Prosecutors have an important role in encouraging civil recovery during early consultation. The City Police, the CPS and private sector recently worked together using specialist powers to achieve the largest ever proceeds of crime forfeiture in the UK. A South African law firm operating from UK offices and a Cypriot registered company both agreed to forfeit €34m to settle litigation alleging that the funds in two bank accounts were from unlawful conduct. By working with partners from Europol, foreign law enforcement agencies and stakeholders from the private sector, including Lloyds Banking Group, the investigation identified overwhelming evidence the monies were unlawfully obtained from international money laundering and layered through the UK banking system to present a veneer of legitimacy. Account Forfeiture Orders were applied for by CPS Proceeds of Crime specialists and the City Police at Westminster Magistrates' Court, which were granted by consent. This was the first time the CPS has used powers under the Proceeds of Crime Act 2002 to appear in court on behalf of the police in an Account Forfeiture Order.

48. Prosecutors can obtain evidence from overseas using mutual legal assistance (MLA). This takes the form of a formal International Letter of Request (ILOR) issued by a designated prosecuting authority or a Court. ILORs, however, are not always effective. Some countries accept and progress and some do not. In addition, CPS and the Home Office (UKCA) are required to carry out risk assessments before requesting evidence from many countries. These assessments mean ILORs cannot be sent in some cases. Quite often this means cases are not progressed by policing and international lines of enquiry continue to frustrate investigations. Aims and objectives of European law enforcement partners can be based on vastly different evidential requirements due differences in legal systems and stances on information sharing which makes collation of evidence more challenging.

49. Obtaining evidence from financial institutions can be challenging. The demand for information and evidence to support fraud investigations is significant and financial institution sources in this area are limited. Pre-order enquiries are most frequently undertaken by accredited financial investigators and many financial institutions have come to expect this. It means that investigators need to rely on already stretched financial investigators to carry out their enquiries which is not the most efficient use of resources. The national register of fraud investigators held by the Economic and Cyber Crime Academy would be a useful way of extending the pool of investigators who undertake regular liaison with banking institutions providing them with confidence in their dealings with policing and assisting the fraud investigative process.

50. In order to request charging advice, the CPS require policing to provide a full evidence file. However, financial institutions are reluctant to provide a witness statement unless legally compelled. This is because there are times when despite vast amounts of time spent preparing statements they have

not been used, and staff who completed the witness statements have been called to attend court across the country only to be told they are not required once they arrive (this is often because the witnesses' evidence is only agreed by the defence at that time). Without the information in an evidential format, it is not evidence against the suspect. This difficulty with getting a witness statement means police are less likely to progress the case. While acknowledging CPS charging decisions have to be made on evidence rather than information a more considered approach to what is required to inform a charging decision would help to address this.

51. Disclosure from financial institutions can be problematic. Normally they will require a court order stipulating exactly what material the officer wishes to view and why. Given the importance of this information to fraud investigations an approach more aligned to applications for communications data and surveillance requests, or another body to authorise banking applications would help to reduce demand on crown courts. This would still provide independence and oversight of applications.

52. The volume of evidential documentation relating to fraud cases is huge. The City Police has millions of pages of evidence relating to ongoing its investigations. The current disclosure system typically adds six months to a medium size investigation. The Attorney General Guidelines 2020 do make provision for the preparation of schedules to continue beyond the point of charge for large and complex investigations where it may not be feasible or necessary to provide schedules at the same time a charging decision is sought due to the quantity and complexity of data to be analysed. However, the position remains that disclosure schedules need to be completed and signed prior to any charging decision.

53. The level of disclosure necessary is decided on a case-by-case basis and is subject to interpretation. Disclosure protocols set by counsel based on the relevancy test are often effective, but dependent upon the views of the judge and the ability of counsel to reach agreements with any disputes, dealt with by applications to the court. Clearer guidance as to what is reasonable and necessary for the disclosure process to be signed off and consideration of disclosure protocols being made a requirement, not an option, would reduce the length and resourcing requirements of fraud investigations.

54. Although there are standard approaches following 2020 Attorney General Guidance, General Data Protection Regulation compliance impacts the disclosure burden in criminal investigations. Counsel often takes a different opinion on the level of redaction required. From treatment of information relating to a co-accused no longer part of a case, treatment of moving images of members of the public in body worn footage to how many digits should be redacted from a telephone number. Early consultation between CPS and counsel to develop disclosure policies concerning the level of redaction and GDPR compliance significantly enhance the prospect of a successful prosecution.

55. The volume of information held on digital devices is substantial and can be duplicated across numerous devices. Although key search word strategies are agreed to limit the amount of documentation that needs to be reviewed, thousands of positive results still need to be reviewed and

scheduled for disclosure. Rules on disclosure require modernisation to take account of bulk data from digital media. Other jurisdictions do not have the same rules regarding disclosure. For example, in a case involving prosecutions in both the UK and Switzerland, the City of London Police had to request, review and disclose the investigation record and transcripts of trial (approx. 50,000 pages) but the Swiss did not need UK papers for its trial.

Sanctions and sentencing

56. Fraud causes serious harm to victims' finances, mental health and emotional wellbeing. In the 2020/21 financial year Action Fraud identified and supported 28 risk-to-life incidents and 234 individuals at risk of suicide or self-harm. Further to this, nearly 340,000 victims who reported to Action Fraud, self-identified as vulnerable, the real number is of course likely to be much larger. In some cases, it results in suicide and self-harm. For example, in October 2020 a key worker who suffered mental health issues committed suicide by jumping onto a motorway following contact by scammers spoofing HMRC that morning. The fraudsters led her to wrongly believing she was in trouble for fraud and owed £18,000. She referenced the calls from HMRC, among other pressures, in her suicide note.

57. There are also long-term financial implications when life savings are lost, and physical and emotional harm from being deceived. Fraud victims have described scams as "financial violence"; the outcome being worse than physical injury. A victim's ability to trust coupled with a feeling of blame and subsequent isolation shifts the discussion away from merely the impact in monetary terms.

58. There is currently an over-reliance on the level of financial loss in the sentencing guidelines. The impact of losing £5,000 to one person can be as impactful as the impact of losing £50,000 to another, depending upon their financial stability. As identified above, harm does not always correspond to financial loss. The sentencing guidelines should allow for a full range of sentencing powers for very high harm but low financial loss. Sentencing guidelines should be updated to provide a mechanism to elevate an offender up the sentencing categories based on their actions contributing to serious emotional or other harm. Sentencing guidelines could also be updated to include other aggravating factors such as hindering recovery of money to the victim. Given the harm caused to individuals by fraud the maximum sentence for fraud (currently 10 years) should be at least in line with the maximum sentence for money laundering (14 years).

59. In 2011, there were attempts to introduce a 50% reduction in sentence for early guilty pleas. This could be revisited for pre-charge admissions in police interview for economic crime offenders as it would save police resources, reduce court time and provide swifter justice for victims.

Best Practice

60. The US statute on criminal corporate liability is broader than the UK's, so companies can more often be held liable for economic crimes there than in the UK. In the US a company can be liable if one of its agents commits a criminal act within the scope of their employment and for the benefit of the corporation. As such, a corporation can be held liable for an agent no matter what their place in the corporate hierarchy and regardless of the

efforts in place on the part of corporate managers to deter their conduct. In the UK, liability requires the identification of the controlling mind of the company. This identification principle acknowledges the existence of corporate officers (e.g. board members and/or senior management) who are the embodiment of the company when acting in its business. Their acts and states of mind are deemed to be those of the company. Criminal acts by such officers will not only be offences for which they can be prosecuted as individuals, but also offences for which the company can be prosecuted because of their status within the company.

61. The USA have some mechanisms/legal gateways to share their investigation findings via Date Sharing Order (DSO). This allows them to expedite an investigation rather than wait for an MLAT which may take up to 6 months or longer.

21 April 2022