Cifas – Written evidence (FDF0015)

Cifas is the UK's fraud prevention community. We are a not-for-profit membership organisation which leads the fight against fraud by sharing data, intelligence and learning. We have over 30 years of experience in fraud prevention and financial crime, working with a range of UK businesses, charities, and public bodies to help protect themselves, their customers and the public. At the time of writing there are over 620 organisations in Cifas membership, and a full list of Cifas members can be found on our public website. We are a Specified Anti-Fraud Organisation (SAFO) designated under the Serious Crime Act 2007 as recognised by the UK Government.

The Cifas National Fraud Database (NFD) is used to share information about fraudulent conduct against member organisations. We call this fraud risk information. An example of this is when someone uses another person's details, such as name and address, to apply for a credit card. The NFD prevents over £1 billion in fraud losses every year.

Our Response

Fraud Landscape

1. What fraud risks are UK a) individuals, b) the Government and c) businesses particularly vulnerable to today, and what are the reasons for this?

i. The common fraud risk which makes individuals, Government and businesses vulnerable to fraud is the abuse of online channels to anonymously facilitate fraud. Fraudsters have become adept at abusing online platforms, whether search engines, social media or job sites. That abuse can range from scam payments for services or jobs that don't exist, to eliciting personal or financial information for identity frauds targeting businesses and Government departments. In targeting individuals through these channels, fraudsters have a better chance of circumventing the range of checks that businesses have implemented to combat fraud.

2. What future economic and technological developments are likely to impact how fraudsters seek to commit crime over the next five to ten years, and how might these be prepared for and mitigated? What role can technology and tech companies play in combatting fraud across this timescale?

i. While economic and technological developments are not easy to predict, the speed at which fraudsters adapt to and exploit these changes is all too predictable. This has been illustrated during COVID, with new support schemes swiftly targeted and scams tailored to the news of the day, such as the vaccine rollout. Increased home working has also been exploited, with more isolated staff targeted through a range of digital channels and platforms, from email to video conferencing services.

ii. A common thread through these frauds, in their various forms, is their reliance upon technology and online platforms, as noted under our answer to question 1. These platforms are exploited at scale, whether through the posting of fraudulent adverts, social engineering via direct messaging, or the sale of data, documents and guidance on how to commit fraud.

iii. We therefore welcome the inclusion of fraud within the Online Safety Bill, for both paid-for adverts and user-generated content, to ensure that appropriate responsibility is placed on major online platforms. The Bill's scope is limited to those major social and search engine platforms, and so it is important that the Online Advertising Programme effectively tackles fraudulent abuse of adverts across other channels, such as job sites, which are so often exploited to advertise jobs that simply do not exist.

3. Is fraud and its victims treated as a priority? If not, what are the reasons for this.

i. Our response is particularly focussed on those high volume, relatively low value fraud cases, which are often not within the remit of the Serious Fraud Office or other agencies, and so often fall between the cracks. In their totality, these cases amount to £ billions lost to victims across both organisations and individuals, which is used to fund wider organised criminality.

ii. For many years Government and law enforcement have only treated high value scams, such as investment scams, as high harm fraud types, and have prioritised these over other types of scams and fraud. This has in part been due to scam losses traditionally being borne by the victim of that scam. This policy has inadvertently provided organised criminals with a green light to commit high volumes of identity fraud, offering big profits and a very low risk of prosecution, against business.

iii. Nearly a million identity frauds have been recorded to the Cifas National Fraud Database alone over the past 5 years:

   a. Every one of these records has been fed into the National Fraud Intelligence Bureau (NFIB) and officially counted within the ONS crime statistics

   b. They represent £ billions in fraudulently obtained funds, that will undoubtedly have been used to fund other types of serious and organised crime

   c. Indeed, highly organised techniques are used to harvest and abuse identity data, from hacking, to phishing, to wider social engineering, as well as buying and selling data, card details and documentation on the dark and surface web

   d. This threat has continued to grow during the pandemic, with over 102,000 identity frauds recorded to Cifas in the first 6 months of 2021, representing an 11% increase year on year

iv. It should be noted that scam victims are increasingly being reimbursed by the relevant financial institutions, including under the APP Scams Voluntary Code. Financial institutions will therefore often be the primary financial loser for both scams and identity fraud, which both create direct harm and concerns for the public.

v. When a member of the public's personal information is abused to commit identity fraud or hijack their existing services, they are often left feeling extremely anxious about what other activity may be taking place under the guise of their identity. It can take months for an individual to repair their credit score and harm to their reputation. The emotional and

financial harm to individuals that have to rectify this damage can equal or even exceed a scam - 'Having my identity stolen cost me £10,000' - BBC News

vi. Identity fraud funds organised crime, which hurts individuals and wider society, from drug dealing, to people trafficking and even terrorism. The UK's response to terrorism and organised crime is driven by the 4 P's - Pursue, Prevent, Protect, Prepare. Pursue to detect and prosecute, Prevent to stop people turning to this criminality, Protect to understand the threat and implement measures to reduce vulnerabilities, and Prepare to mitigate the impact of an attack. It is vital that this approach is applied to the government and law enforcement response to fraud, given the level of organisation, sophistication and enablement of terrorism itself.

vii. This article provides details on how financial fraud, including identity fraud, is being used to fund terrorism - with documented links between fraud and terrorism going back to the IRA, funded by tax fraud, and on to al-Qaeda who often receive funding via credit card fraud.

'However, fraud has now become the crime of choice for terrorists who have acquired funding via benefit and credit card fraud, identity theft and the sale of counterfeit goods.'

viii. If OCGs and terrorist groups didn't use false documentation and only used their own banks accounts, for example, it would be far easier to link their activities and apprehend the offenders. This not being the case makes identity theft and fraud a key enabler for organised crime, including terrorism.

ix. This is a key reason why tackling fraud against businesses is so crucial and should not simply be dismissed as losses that financial institutions can afford to absorb.

4. What is the role of international actors in the UK's fraud landscape? What are the barriers to tackling borderless fraud? Not answered

Action to Tackle Fraud

5. How effective is the current structure for policing fraud? How successful are the City of London Police, including Action Fraud and the National Fraud Intelligence Bureau, at executing their role as the lead police force for fraud?

i. We see opportunities for both top down and bottom up changes, that can deliver a far more effective and co-ordinated response to fraud across government and law enforcement.

ii. A single dedicated national strategy to tackle fraud, to deliver a co-ordinated inter-agency response across Home Office, NECC, law enforcement and wider partners

   a. Identity fraud and wider fraud against organisations must be given equal billing to scams within this strategy

   b. The strategy should drive a joined up response across agencies, that works towards the same objectives - not parallel plans that may clash or duplicate, as is often the case presently

iii. Linked to that national strategy, fraud should be made a policing priority across forces - not just for City of London Police as lead force and units that are funded by industry.

   a. There should be ring-fenced funding within forces to tackle fraud - avoiding resource drain to other areas of activity and the current erosion (in some instances decimation) of dedicated fraud units

   b. Specialist skills and training is required to deliver a range of law enforcement responses to tackle fraud more effectively. This should include

      - Training for officers and civilians that helps deliver a suite of responses, from investigations to disruption of online platforms and marketplaces enabling fraud, to partner work that delivers legal, proportionate data sharing
      - More specialist police investigative staff who understand the fraud problem, and work more closely with the thousands of skilled fraud investigators employed in the private sector and wider public sector
      - As resourcing and skills improve, so will the understanding of how best to tackle volume fraud, in all its guises, and maximise harm reduction

iv. The above changes, if implemented, have a run-up time, and in the meantime, fraudsters will continue to operate, draining businesses and the public purse and funding organised crime. Law enforcement should therefore be making use of the information, data, resource and partners that they have at their disposal currently.

   a. There are millions of industry fraud risk records held by law enforcement, not currently being utilised, that could be analysed and interrogated to add value across intelligence, investigation and the disruption of fraud and wider crime

   b. Law enforcement should interrogate, investigate and build-up their limited understanding of identity fraud networks and their links to wider crime. From this, informed deliverables, measurables and targets can be developed around identity fraud, to maximise harm reduction. Focussing on scams alone is simply not justifiable given the direct and indirect harm from identity fraud

   c. Data and intelligence from law enforcement investigations and criminal debriefs must be shared to empower organisations to help prevent and detect fraud. This should be a requirement of policing, not an optional that is seldom pursued, as is currently the case.

6. Are sufficient resources available to Government organisations (such as the Serious Fraud Office and Crown Prosecution Service) and wider police forces to tackle fraud and support victims, and how should this be addressed if not? Answers need not be limited to financial resources.

i. The latest crime statistics shine a harsh light on the gap between the vast scale of fraud and the tiny proportion of police funding dedicated to fraud. It is scandalous that fraud accounts for nearly 50% of all crime, and continues to grow, but just 2% of all police funding is allocated to tackling fraud.

ii. Too often other crime types are used as an excuse for not better resourcing the fight against fraud, when in fact fraud both funds and enables other serious and organised crime types, from people trafficking and human slavery, to terrorism. Indeed, little organised criminality could be carried out without identity fraud to provide access to fraudulent funds, accounts and documentation.

7. What are the responsibilities of the private sector in protecting the public against digital fraud? How can a balance be achieved between the need to tackle digital fraud whilst supporting the growth of these sectors? To what extent is work done to combat fraud across the private sectors undermined by siloed or independent working practices?

i. As per our answer to question 2, we welcome the responsibility being placed upon major online platforms to combat fraud, through the Online Safety Bill. Organisations within financial services have long had to balance growth and commercials with tackling fraud and meeting their regulatory requirements, and online platforms should be no different. Financial services has also voluntarily shared data to combat fraud, across sectors, for decades, and we hope to see this example followed by both technology companies and those parts of the public sector that are still not sharing fraud risk data cross sector.

8. What are the legislative or regulatory impediments to sharing fraud risk data across and between the private and public sectors? For example, to what extent does General Data Protection Regulation (GDPR) limit data sharing?

i. The Digital Economy Act has been used to conduct a number of pilot data sharing exercises between public authorities. While we support those pilots, the act has created some confusion around existing legal provisions which enable public authorities to not only share data with each other, but also the private and third sectors.

ii. Section 68 of the Serious Crime Act 2007 provides a power for a public authority to disclose information as a member of a specified anti-fraud organisation (SAFO) or otherwise in accordance with arrangements made by such an organisation, for the purposes of preventing fraud.

iii. A key driver for the serious crime act provisions was the problem many public authorities were having, in determining definitively whether they could or could not share data for fraud prevention purposes, including with the private sector. The Serious Crime Act provisions therefore provide neat and clear primary legislation, confirming that any public body can share with a SAFO for fraud prevention purposes. Cifas is a SAFO, as designated by the Home Office, and many public authorities - across both central and local government - are in Cifas membership and utilising the gateway to participate in our cross sector data sharing schemes.

iv. There is however a lack of awareness in some areas of government around the gateway, which can lead to confusion, act as barrier to sharing and an over-reliance on pilots through the Digital Economy Act. The importance of all public authorities using these provisions could not be more relevant given the £ billions lost to fraud through abuse of COVID schemes, with the need for better checks and sharing highlighted by the PAC Inquiry on COVID. It is therefore not the legislation or regulation that

is creating the barrier, but inadequate awareness, focus and usage of a tailor-made legal gateway for public-private sharing.

v. We therefore propose that the Serious Crime Act provisions are more strongly backed by Government.

9. What is the role of the individual in relation to fraud? Are consumers well informed about the risks of fraud and how to prevent them? If not, which bodies or organisations should do more to ensure this? What are the most effective methods of educating the public about fraud crime and prevention?

i. There is no silver bullet that will enable individuals to not be duped by fraudsters, and research shows that individuals can still fall foul of these crimes even when they have seen guidance which flags key warning signs. That said, timely and clear guidance is crucial to helping combat fraud, and we work with our partners in the landscape to help provide joined up and consistent advice and messaging.

Legislative Remedies

10. What is your assessment of the Fraud Act 2006? What has been the impact of the Act and is it having any unintended consequences; if so, what are these?

i. The Fraud Act 2006 provided the required clarity around what constitutes fraud, by removing the confusing barrier of conspiracy and introducing a general offence covering false representation, failing to disclose information and abuse of position.

ii. Our assessment is that the Act has provided police and law enforcement with the legal clarity they require to tackle fraud more effectively, including for prosecution. It is therefore not deficiencies in the Fraud Act that has led to shortfalls in the Government and policing response to fraud, but a lack of focus, prioritisation and investment, as outlined in detail under our response to questions 3 and 5.

11. Is existing legislation effective in tackling the increase in modern forms of fraud? If not, is there a legislative remedy, or should fraud be addressed primarily through implementation of existing provisions?

i. Modern fraud is most frequently conducted online, at speed and in high volumes. It is therefore critical that organisations are equally agile, and share data in real-time across sectors, to combat fraud at all points of the customer journey. There are well established systems and legal gateways to enable this, including legitimate interest provisions within GDPR/DPA for fraud data sharing.

ii. There is however, as acknowledged by Government in the recent DCMS consultation, Data: A New Direction, an issue around clarity of wording in GDPR/DPA, which can lead to a lack of confidence in utilising legitimate interests for data sharing. We have seen this directly, with some organisations - particularly in the public sector - lacking clarity around the balancing test and its application, and then not having confidence to share data that could have prevented fraud and significant harm.

iii. This confusion and lack of confidence is also leading to consent being used as a fall-back by some organisations, including government agencies,

even in instances where this renders the fraud prevention measure almost completely redundant of value. For example, enabling an applicant to pick and choose the specific fraud and identity verification checks that are to be conducted, such as checking document details against the records held by the issuing government agency. The end result is that those presenting a false document can choose to avoid that check and will instead present another form of documentation where they believe they are less likely to be caught.

iv. We therefore support the suggestion by Government, within Data: A New Direction, to remove the balancing test and to create a limited, exhaustive list of legitimate interests for which organisations can use personal data without applying the balancing test. That list of activities must include the prevention and detection of fraud, AML and wider financial crime.

12. Is the current system in place for prosecuting fraud cases working effectively? If not, what are the key barriers to prosecution? Not answered

13. Are sanctions and penalties for criminals who commit fraud an effective deterrent against future criminal activity, and if not, what might be more successful?

i. While we believe longer sentences for fraudsters would help provide a greater deterrent, this can only be effective if married with a greater number of police investigations and prosecutions, across the full range of fraud types. Without that uplift in investigations and prosecutions there is little deterrent to criminals conducting fraud, as they know there is a such a remote chance they will ever be investigated, let alone prosecuted and facing jail time. This is particularly true of those fraud types outside of scams, including frauds against business and identity fraud, which are so rarely investigated by police that virtually no deterrent exists.

Best Practice

14. What lessons can be learned from effective policy interventions and schemes both in the UK and overseas?

i. There are industry standard fraud checks used by hundreds of organisations, spanning private, public and third sectors, to share data, intelligence and learning to prevent and detect fraud. This sharing, on a non-competitive basis, helps protect the public and organisations from fraud, and prevents £ billions entering the criminal economy and being used to facilitate other types of organised crime. There are therefore existing best practice solutions, utilising well established legal gateways, available to organisations.

ii. These solutions are used comprehensively across financial services and also by some central and local Government departments. There are, however, gaps in the use of these solutions within the public sector, including some of the largest Government departments responsible for collecting and administering hundreds of billions of pounds. The failure to undertake these checks for COVID support schemes highlighted this long-standing issue, with £ tens of billions lost from the public purse and put into the hands of organised criminals. Government departments must learn these lessons and start undertaking these industry standard fraud checks.

15. Can you suggest one policy recommendation that the Committee should make to the Government?

i. For the reasons outlined under question 14, we would propose mandating industry standard fraud checks for Government departments, including but not limited to the largest central Government departments.

ii. These checks have the power to help identify frauds at the point of application and throughout the customer life cycle, and also recover public funds where fraudulent payments have already been made. The level of losses to the public purse, combined with the harm to individuals from the organised crime the frauds fund, makes mandating these industry standard checks, crucial.

iii. It should be noted that while, as we understand it, the new Public Fraud Authority will look to develop a minimal level of 'fraud proofing' before

new large central Government projects are launched, this will not include HMRC or DWP, nor existing solutions. The need for industry standard fraud checks to be mandated for Government departments therefore remains.

20 April 2022