House of Commons

Justice Committee

Fraud and the Justice System: Government Response to the Committee's Fourth Report of Session 2022–23

Sixth Special Report of Session 2022–23

Ordered by the House of Commons
to be printed 10 January 2023

HC 1020
Published on 11 January 2023
by authority of the House of Commons

Justice Committee

The Justice Committee is appointed by the House of Commons to examine the expenditure, administration and policy of the Ministry of Justice and its associated public bodies (including the work of staff provided for the administrative work of courts and tribunals, but excluding consideration of individual cases and appointments, and excluding the work of the Scotland and Wales Offices and of the Advocate General for Scotland); and administration and expenditure of the Attorney General's Office, the Treasury Solicitor's Department, the Crown Prosecution Service and the Serious Fraud Office (but excluding individual cases and appointments and advice given within government by Law Officers).

Current membership

Sir Robert Neill MP *(Conservative, Bromley and Chislehurst)* (Chair)

Rob Butler MP (*Conservative, Aylesbury*)

Angela Crawley MP (*Scottish National Party, Lanark and Hamilton East*)

Janet Daby *(Labour, Lewisham East)*

James Daly MP (Conservative, Bury North)

Maria Eagle MP (*Labour, Garston and Halewood*)

Kate Hollern MP (*Labour, Blackburn*)

Paul Maynard MP (*Conservative, Blackpool North and Cleveleys*)

Dr Kieran Mullan MP (*Conservative, Crewe and Nantwich*)

Edward Timpson MP *(Conservative, Eddisbury)*

Karl Turner MP (Labour, Kingston upon Hull East)

Powers

The Committee is one of the departmental select committees, the powers of which are set out in House of Commons Standing Orders, principally in SO No 152. These are available on the internet via www.parliament.uk.

Publication

Committee reports are published on the Committee's website at www.parliament.uk/justicecttee and in print by Order of the House.

Committee staff

The current staff of the Committee are Robert Cope (Clerk), Philip Jones (Second Clerk), Anna Kennedy-O'Brien (Committee Specialist), Tanya Lightfoot-Taylor (Committee Specialist), Su Panchanathan (Committee Operations Officer), George Perry (Committee Media Officer), Jack Simson Caird (Deputy Counsel), and Melissa Walker (Committee Operations Manager).

Contacts

All correspondence should be addressed to the Clerk of the Justice Committee, House of Commons, London SW1A 0AA. The telephone number for general enquiries is 020 7219 8196; the Committee's email address is justicecom@parliament.uk.You can follow the Committee on Twitter using @CommonsJustice.

Sixth Special Report

The Justice Committee published its Fourth Report of Session 2022–2023, *Fraud and the Justice system* (HC 12), on 18 October 2022. The Government's Response was received on 16 December 2022 and is appended to this report.

Appendix: Government Response

Introduction

This is the Government's response to the Justice Select Committee report 'Fraud and the Justice System' (HC 12) published 18 October 2022. The report made a total of 18 recommendations around several topics including the Government's commitment to tackle fraud; supporting victims; working with industry and, investigating; prosecuting and disrupting fraud.

Overview

The Government is grateful to the Justice Select Committee and all those that provided evidence for their report. Tackling fraud requires a unified and co-ordinated response from government, law enforcement and the private sector, to better protect the public and businesses, reduce the impact of fraud and increase the disruption and prosecution of fraudsters. We welcome the report and thank the Committee for the recommendations they have made.

The Government has carefully considered the evidence, findings and recommendations of the report and set out our response to its findings below. For ease, these have been numbered in line with the Conclusions and Recommendations of the report itself.

Government ambition and accountability

Background

Fraud is a growing issue and one which does not sit naturally with the other elements of the Minister for Security and Borders extensive portfolio. (Page 37, Paragraph 3)

Recommendations

Fraud and other forms of economic crime need to sit within a Ministerial portfolio that allows the postholder to prioritise this increasingly important area of work, and who can draw together parts of government and private sector companies to create a unified approach to tackling fraud. This should also be in such a way as will give the issue more publicly visible political and governmental ownership and accountability. (Page 37, Paragraph 4)

Government Response

Tackling fraud is a priority of the Government and given the overlap between economic crime and national security, the Security Minister is well positioned to provide leadership, ownership and oversight of the Government's response to fraud against businesses and individuals. The successful relaunch of the Joint Fraud Taskforce is testament to the role of the Security Minister, as a Home Office minister, to bring together key stakeholders in both the public and private sectors to combat fraud.

Victims

Background

Fraud crimes do not impact victims equally and due to limitations in victim support capacity, efforts to support victims of fraud should be focused on those who need it most. It is therefore vital that responders to these crimes have the training and experience required to identify who may need further support and can direct them to services which can provide this aid. (Page 37, Paragraph 5)

Support available for victims of fraud is patchy and inconsistent. Thirty-seven police forces currently work with victim care units. However, this is not compulsory and there is currently no national standard for fraud victim care. (Page 37, Paragraph 6)

Recommendations

The Government should set a minimum standard of care that a victim of fraud can expect to receive when reporting a crime and ensure that all 43 police forces in England and Wales are working with victim care units to provide victims with effective support by the end of 2023. (Page 37, Paragraph 7)

Government Response

The Government agrees that it is imperative that all victims of fraud receive enough support and advice. To ensure this standard is met, the Home Office are working with the City of London Police (CoLP) to expand National Economic Crime Victim Care Units (NECVCU) across England and Wales from 2023, for victims whose cases are not investigated by the police. The NECVCU will help victims feel more confident and aims to significantly reduce the likelihood of repeat victimisation.

All 43 forces recognise the need to provide support and do already deliver victim care, whether it is locally delivered and commissioned, or alongside the NECVCU. The NECVCU service has now been rolled out to a total of 37 forces at Level 1 (non-vulnerable victim care) and 6 forces at Level 2 (vulnerable victim care). From April 2023, NECVCU will cover 40 out of 43 forces at Level 1 and 34 out of 43 forces at Level 2. We continue to work with the remaining forces to ensure all 43 forces have a consistent approach to supporting all victims of fraud and cyber-crime.

More broadly, the Government is introducing a Victims Bill that will improve the experiences of all victims of crime, including victims of fraud. Enshrining the Victims'

Code in law will send a clear signal about what victims can and should expect from the criminal justice system. We are also strengthening oversight of how criminal justice agencies treat victims so that we can identify problems and drive up standards.

The Code of Practice for Victims of Crime sets out the services and a minimum standard for these services that must be provided to all victims of crime, including victims of fraud. Under the Code victims are entitled to referral to support services for victims, including specialist services where appropriate. [Information about what is available specifically for victims of fraud is on the Action Fraud website: https://www.actionfraud.police.uk/]. Local support services funded by Police and Crime Commissioners can also be accessed without the victim reporting the crime. Under the Victims' Code, victims are also entitled to be told when key decisions on the investigation are made and, where applicable, to have the reasons behind these decisions explained to them.

Action Fraud 1.1

Background

Many victims of fraud find it difficult to know how to report the crime. It needs to be made much clearer to victims how they can report a crime, as the current lack of clarity brings added distress to the process. We acknowledge that increasing awareness of Action Fraud will place increased pressure on the already stretched reporting service, but it is vital that victims feel able to report their crimes both for the individual to feel that they are being listened to, and also to help build a national picture of fraud crimes. (Page 37, Paragraph 8)

Recommendations

The Government should increase efforts in advertising Action Fraud to raise public awareness of how to report incidents of fraud. (Page 38, Paragraph 9)

Government Response

Action Fraud have developed a calendar of campaign activity, underpinned by data and insight, to encourage reporting to the service, increase public confidence and impact behaviour. So far in 2022, Action Fraud and Cyber Protect have delivered a total of 7 national campaigns and have collaborated on or helped to amplify national campaign activity from a host of partners, including the National Economic Crime Centre (NECC), National Crime Agency (NCA) and Financial Conduct Authority (FCA).

More broadly, the Government recognises the importance of empowering the public through high quality communications, such that the public can better protect themselves against the threat from fraud. We will set out further details of the approach in the upcoming fraud strategy.

Action Fraud 1.2

Background

Individual police forces do not have the capacity to manage the volume of fraud reports made and so it is vital that there is an effective reporting service that is victim-focused and can deal consistently with reports and progress cases swiftly to a resolution, all while keeping the victim updated on the actions being taken. Action Fraud has not proved itself to be fit for these purposes and is not sufficiently resourced to meet the growing and varied challenges of fraud. Action Fraud is due to be replaced in 2024; however, victims should not have to wait until then before they begin to see an improvement to the mechanisms for reporting fraud and monitoring the progress of their cases. (Page 38, Paragraph 10)

Recommendations

The Government should take steps now to address these issues. (Page 38, Paragraph 10)

Government Response

The Government agrees that victims of fraud should have access to an effective reporting service, alongside the support and information they require and therefore, we are replacing Action Fraud in 2024. Victims, however, will not have to wait until then before they begin to see an improvement to the mechanisms for reporting fraud and monitoring the progress of their cases. We are providing £30 million to City of London Police (CoLP) over the next three years, to support the upgrade in the Action Fraud service. A number of improvements to the existing system have already been put in place, as part of this upgrade, to improve the victim reporting experience and the quality and timeliness with which cases are sent to police forces for action.

Improvements include:

- Increasing the number of staff in the call centre
- Expanding the reach of victim care services
- Using automation to increase effectiveness
- Sending cases to forces faster

One key improvement, currently underway, is to transform the Action Fraud website where the public can report fraud and cybercrime. In 2023, a new, user-friendly, accessible reporting tool and website will be launched, offering an improved victim experience and simpler pathways to access further support and guidance. It will crucially improve: the ease of reporting; quality and validation of data; timeliness of the reports from the public; and provide law enforcement the intelligence they need to investigate and disrupt more fraudsters.

Action Fraud 1.3

Background

Although the level of staffing at Action Fraud's reporting call centre has increased from 75 to 95, this is clearly not sufficient to provide an adequate service to all those reporting a fraud. *(*Page 38, Paragraph 11)

Recommendations

Sufficient staffing needs to be put in place to ensure Action Fraud and its successor service can provide a high-quality service to victims, keeping them updated on the progress of their case and directing them to appropriate support services where required. (Page 38, Paragraph 12)

Government Response

It is important to ensure that victims get through to call centres as quickly as possible, and this is one of the key improvements we are working towards. This may require more staff, or it may require better use of technology. We will work to ensure there is sufficient capacity with the new commercial suppliers once appointed.

In the meantime, we will be launching a new reporting tool and website next year. This tool will improve the ease and timeliness of the reporting experience, as well as offering simpler pathways to access further support and guidance. To complement this, a new automated SMS feature will send victims waiting in a call queue a direct link to the new website as an alternative reporting option and a new chat bot has been developed for the website to handle greater volumes of reports.

Action Fraud 1.4

Background

We welcome the Government's plans to replace Action Fraud with a new service in 2024; however, we understand from the Government's evidence to our inquiry that the planned changes are focused on the technology underpinning the service, primarily improving the analytical tools applied when a crime is reported rather than improving customer experience. While this is an important development, changes to the service also clearly need to bring about improvements in the victim's experience of reporting a fraud crime. (Page 38, Paragraph 13)

Recommendations

While we welcome the Government's commitment to replace Action Fraud with a new service better able to record and disseminate information about a crime, the service also needs to focus on victim experience, ensuring there are trained individuals staffing Action Fraud's successor who can assess the needs and vulnerabilities of victims and direct them to appropriate resources. (Page 38, Paragraph 14)

Government Response

The Government agrees that we need to ensure that victims receive the support they need when reporting a fraud. To achieve this, we are providing over £30 million to CoLP, over the three years, to support the upgrade in the Action Fraud service and a number of improvements to the existing system have already been put in place to improve the victim experience. This includes the latest introduction of the Action Fraud Chat Bot.

An overhaul of Action Fraud and creation of a modern victim experience focused reporting tool and website, in 2023, will offer simpler pathways to access further support and guidance. These improvements, which have been tested across the victim support landscape, law enforcement agencies, and other relevant bodies, will help to improve victim experience and satisfaction and, potentially, reduce repeat victimisation. By 2024, the whole service will be refreshed leading to greater outcomes for victims. The new service will also provide focussed and targeted support to victims through the AF National Economic Crime Victim Care Unit (NECVCU) service. This service has been rolled out to 37 forces and supported over 240,000 victims since its inception.

Compensation

Background

We are wary of placing too great an emphasis on the compensation of victims. We do not want to give criminals carte blanche to commit their crimes just because victims can be reimbursed, since their crimes will continue to have a significant financial impact on the UK economy, as well as millions of banking customers, even if these losses are not borne by the defrauded individuals directly. The main focus should be on ensuring these crimes are prevented where possible; however, maximising the recovery of assets for victim compensation should be a priority for investigatory bodies once they become aware of a crime having taken place. (Page 38, Paragraph 16)

Recommendations

The Government should introduce changes to compensation order legislation to allow for flexibility in altering the order value if a criminal is later found to have assets of greater value which can be used to compensate victims of their crimes. This would bring practice into line with that already in place for the amendment of confiscation orders to allow for increased asset recovery. (Page 38, Paragraph 15)

Government Response

The Government acknowledge this important issue of whether the court should be able to increase the amount of an existing compensation order made in connection with confiscation proceedings, similar to the way it can already increase the amount payable under a confiscation order, should there be evidence of further benefit from the criminal conduct concerned.

We are recovering more criminal assets than ever before: £354 million was recovered from the total proceeds of crime in 2021/22, 61% higher than the previous year. However, we recognise there is more to be done to strengthen the law. In 2018, the Government

asked the Law Commission to review this part of the law in detail. On 8 November 2022, the Law Commission published a detailed review of Confiscation proceedings, including compensation during confiscation proceedings. We will consider this issue further to decide what legislative reforms are needed to improve confiscation.

Investigating Fraud 1.1

Background

Within policing, there are various chains of command when it comes to tackling fraud cases, with investigations being conducted at a local level but with central bodies, namely the City of London Police and the National Economic Crime Centre, having responsibility for the overall approach to combatting fraud. This can create confusion and lead to the passing of responsibility for fraud cases between forces and other police organisations. (Page 39, Paragraph 17)

Recommendation

The Government should ensure agreements are in place between the City of London Police, the National Economic Crime Centre, and local police forces to outline responsibilities in relation to fraud and also highlight the support available to local forces working within fraud from centralised bodies. (Page 39, Paragraph 18).

Government Response

How these organisations interact is set out in a number of places, including the National Lead Force for Fraud Agreement and the National Fraud Policing Strategy 2019, which set out the strategic framework, through which the City of London Police, National Economic Crime Centre, local forces and other law enforcement partners work collaboratively to tackle fraud. Further detail will be included in the Government's Fraud Strategy that will be published shortly.

The City of London Police (CoLP) is the National Lead Force for fraud, and the portfolio lead for economic and cyber crime. Their responsibilities are set out on GOV.UK. CoLP provides support to investigative teams nationally through the promotion of best practice, training and professional development, as part of its Economic and Cyber Crime Academy.

The National Economic Crime Centre (NECC), supported by CoLP, is the whole system lead responsible for allocating cases to local and regional economic crime teams. These interorganisational links will be strengthened by the establishment of a national law enforcement network to tackle fraud.

Investigating Fraud 1.2

Background

Fraud is not an investigative priority for police forces, partly because it is not a crime type for which forces are held accountable for their performance. Fraud statistics are not included in local and regional performance data despite most of these crimes still being

investigated at the local and regional level. Without this data it is impossible to identify weaknesses in the response to these crimes and boost investigations of fraud crimes. (Page 39, Paragraph 19)

Recommendation

Fraud should be made a Strategic Policing Requirement to focus effort and resources on combatting this crime type. Additionally, performance data should be collected, monitored, and published at local and regional levels, as is done for other crime types, to ensure law enforcement bodies are held accountable for their progress in tackling fraud. (Page 39, Paragraph 20)

Government Response

The Strategic Policing Requirement (SPR) is the document that sets out what, in the Home Secretary's view, are the national threats at the time the document is issued, and the national policing capabilities required to counter those national threats. The current SPR (published in 2015[1]) includes Serious and Organised Crime as a national threat and explicitly references fraud within that – although we recognise feedback from many sides that this reference is not enough. Home Office ministers are currently considering a revised SPR and we are hopeful any new SPR will be stronger on fraud capabilities.

Regarding performance data, the Action Fraud website provides details of judicial outcomes for fraud and cyber-crime broken down by police force and other agencies in the UK, for 1 April 2019 to 31 March 2020. The National Fraud Intelligence Bureau (NFIB) and cyber-crime dashboard also provides a breakdown of fraud data by force area. More information on Action Fraud data can be found using the following link: https://www.actionfraud.police.uk/fraud-stats.

Investigating Fraud 1.3

Background

Fraud accounts for more than 40% of all crime yet receives only around 2% of police funding. Out of the 20,000 new police officers being recruited, only 380 are planned to be deployed in the response to fraud. If the Government is serious in its ambition to reduce fraud, it needs to ensure it is allocated sufficient resourcing within police budgets to help identify and prosecute crimes as well as prevent these crimes from occurring. (Page 39, Paragraph 21)

Recommendation

The Government needs to put in place sufficient funding and police resourcing to bring about a step-change in the response to fraud. (Page 39, Paragraph 22)

1 Link here: strategic policing requirement (publishing.service.gov.uk)

Government Response

The Government is increasing law enforcement investigative capacity to tackle fraud. Over the next three years the Spending Review has allocated £400 million in tackling economic crime, including fraud. This is in addition to the funding that the Home Office commits each year to the NECC in the NCA, and police forces, including over £15m each year to CoLP as the national lead force for fraud.

As part of the Police Uplift Programme, 725 posts have been dedicated to tacking Serious Organised Crime including fraud. Police and Crime Commissioners and Chief Constables will decide how to allocate further resource they receive through the Programme within their forces. Having piloted new fraud investigation teams in four Regional Organised Crime Units (ROCUs), we are expanding these and rolling them out across all ROCUs.

The Government is also increasing law enforcement investigative capacity in the CoLP and establishing a new fraud investigative function in the NCA as part of the establishment of a national law enforcement network tackling fraud.

Given the nature of fraud and the scale of the challenge to tackle it, the Government recognises that increasing law enforcement resource alone will not be sufficient and that private sector partners will need to play a significant part in combating this crime.

Investigating Fraud 1.4

Background

Fraud crimes can be easy to spot in many cases if a police officer has adequate awareness of technological developments but can be missed in the absence of such knowledge. The training of police remains focused on more traditional crime types whereas there is clearly a need for it to keep pace with the changing nature of offending. (Page 39, Paragraph 23)

Recommendation

The College of Policing should conduct a review of the training offered to frontline staff to ensure it reflects the changing crime landscape and provides a strong foundation in crimes that exploit technology such as fraud. (Page 39, Paragraph 24)

Government Response

The Government is supportive of College of Policing's (CoP) desire to ensure police professionals have access to high standards of learning and professional development, to equip those who might deal with fraud with the right skills and knowledge. CoP are working with the national policing lead City of London Police to review policing arrangements for fraud.

Currently, there are four key strands of fraud training: for new entrants to the service in the recruits' curriculum; general investigation training through the professionalising investigation programme; specific learning products available through the City of London Police Economic and Cyber Crime Academy; and content from the College of Policing's Digital Intelligence and Investigation suite.

The curriculum for all new starters includes curricula on digital investigations, understanding the digital crime scene and recovery of digital material. This is supported by content which helps new and serving officers, police staff and volunteers to acquire the digital skills they need to undertake investigations effectively.

The Government acknowledges that there is more to be done to ensure Law Enforcement have the training they need to effectively combat fraud. We continue to support CoP, as they bring together forces and experts to share best practice and develop collaborative plans for policing to improve their work to detect, prevent and disrupt fraud.

Prosecuting Fraud 1.1

Background

We have heard compelling proposals for dedicated economic crime courts to ensure there are judges with the right skills to oversee what can often be lengthy and sometimes complex cases. This would also help address the backlog in fraud cases, which are not always seen as a priority for listing. We support the steps the Government is taking in this direction. (Page 40, Paragraph 25)

Recommendation

The Government should work with the Judiciary to pilot the establishment of economic crime courts. If the pilots are successful, these types of court should be established around the country to reflect the geographic diversity in the crimes being perpetrated. (Page 40, Paragraph 26)

Government Response

The Government recognises the impact that delays to justice, exacerbated by the Covid-19 pandemic, have on victims, witnesses and defendants, including in fraud cases. We are committed to making sure there is an efficient and effective criminal justice system that is equipped to deal with the challenges of fraud cases and addressing the outstanding caseload as quickly as possible.

The best way to manage existing resource and support fraud cases is to ensure the Crown Court is running as efficiently as possible and reduce the overall backlog quickly. We have removed the limit on sitting days in the Crown Court for the second year in a row, extended Magistrates' courts sentencing powers from 6 to 12 months for a single Triable Either Way offence and are recruiting up to 1,100 judges in 2022/23.

Establishing courts dedicated to economic crime would not in itself increase overall capacity given current numbers of judges. Without this overall increase in capacity, judges would have to de-prioritise other cases, including those with vulnerable victims.

His Majesty's Courts and Tribunals Service continue with the planned construction of the City of London Law courts, an 18-room court located on Fleet Street. Scheduled to open in 2026, this new court will consist of eight Crown, six Civil and four Magistrates' courtrooms. Due to the court's location in London's financial centre, we expect the court will focus on high-level fraud, cyber and economic crime.

Prosecuting Fraud 1.2

Background

Our inquiry heard of problems with the application of disclosure rules which can result in significant amounts of police and prosecution time being spent redacting and disclosing vast amounts of material that turns out to be unnecessary to the case eventually pursued. We are not convinced that the underlying disclosure legislation is the problem but rather there needs to be clearer guidelines on how this legislation should operate in cases with significant amounts of digital material. (Page 40, Paragraph 27)

Recommendation

The Attorney General should review the current disclosure guidelines and consider whether there is merit in introducing specific guidance on disclosure in fraud cases with large quantities of digital material. (Page 40, Paragraph 28)

Government Response

Effective disclosure of unused material remains a crucial part of a fair trial and is essential to avoiding miscarriages of justice. However, the Government recognises that disclosure remains one of the most complex issues in the criminal justice system, particularly in cases with significant amounts of digital material.

The 2018 Attorney General Review of disclosure in the criminal justice system highlighted significant concerns with the culture around disclosure, engagement between relevant parties (prosecutors, investigators, and defence practitioners), and the challenges of modern technology. Following the review, the Guidelines were revised and published in December 2020.

In May 2022, the Attorney General's Office published the first annual review of the Disclosure Guidelines, which concluded that the current Guidelines are a functional and effective tool, but noted that future work may be needed to revisit disclosure in complex crime. Further amendments were made to the Guidelines in order to deliver improvements.

We continue to work closely with operational partners to consider how further improvements can be made. The forthcoming fraud strategy will detail our aim to ensure the disclosure regime meets the needs of complex fraud cases.

Prosecuting Fraud 1.3

Background

The loss of a comparatively small amount of money can have a greater impact on one individual than the loss of a greater amount on another. The current sentencing guidelines do not recognise this and therefore overlook the emotional and psychological impact that fraud crimes can have on their victims. (Page 40, Paragraph 30)

Recommendation

Sentencing guidelines should be amended to give greater consideration to the emotional and psychological harms caused by fraud crimes alongside the financial losses incurred. (Page 40, Paragraph 31)

Government Response

The independent Sentencing Council is responsible for developing sentencing guidelines. It is therefore for the Council to consider the response to this recommendation. We confirm we have shared the report with the Office of the Sentencing Council.

Disrupting and Preventing Fraud 1.1

Background

Our inquiry has repeatedly heard that the most effective way to tackle fraud is to prevent it occurring in the first place. This requires co-operation across the private and public sectors, with the Government using its convening power to unite stakeholders around the ambition to reduce fraud. The relaunch of the Joint Fraud Taskforce is a good start, bringing stakeholders together to discuss a common approach to fraud, and the Committee welcomes the intention to produce a new Fraud Action Plan. (Page 40, Paragraph 3)

Recommendations

Government should continue to bring together the public and private sectors and ensure that the upcoming Fraud Action Plan sets out its ambition for tackling fraud, how this will be achieved, and the roles and responsibilities each industry has within a unified response to fraud. (Page 41, Paragraph 33)

Government Response

The Government agrees that tackling fraud requires a unified and co-ordinated response from government, law enforcement and the private sector to better protect the public and businesses from fraud, reduce the impact of fraud on victims, and increase the disruption and prosecution of fraudsters. The Home Office continues to drive forward this collaboration by convening public and private sector partners through the Joint Fraud Taskforce, which last met on 21 November 2022.

The Government will shortly publish a new strategy which will detail how we will: stop fraud attempts so that people don't lose money; empower potential victims to recognise and avoid fraud; and prosecute far more fraudsters.

We will work with industry to remove the vulnerabilities that fraudsters exploit; with intelligence agencies to shut down fraudulent infrastructure; with law enforcement to identify and bring the most harmful offenders to justice; and with all partners to ensure that the public have the advice and support they need.

Disrupting and Preventing Fraud 1.2

Background

We acknowledge that telecommunications and tech companies are taking steps to improve their response to fraud, however they remain platforms through which the majority of frauds impacting the general public are conducted. There still appears to be a lack of engagement on this subject from those sectors, not least amongst the telecommunications companies. Fraudsters may be using increasingly sophisticated technologies and methodologies to conduct their crimes, but we are not convinced that the largest companies in those sectors do not have the capabilities to increase their efforts to tackle these changes and prevent frauds, particularly in paid-for advertising, from appearing on their systems. Fraud may not have a significant impact on the bottom-line of those companies, however they have a duty of care to their users to ensure everything possible is being done to design frauds out of their systems in order to protect the public. (Page 41, Paragraph 34)

Tech and social media companies have a vital role to play in designing fraud out of their systems to help prevent so many frauds from being conducted online. (Page 41, Paragraph 35)

Recommendation

The Government should prioritise putting in place charters with the social media and tech companies to capture their commitments and responsibilities in relation to tackling fraud, and to enable them to be held to account by government for their progress in this respect. (Page 41, Paragraph 36)

Government Response

The Government agrees with the recommendation of the Committee that further charters, including with social media and tech companies, are an important programme of work. The Home Office is intending to launch a tech and online charter with industry, next year, which will include public and private actions that will drive down fraud in these sectors and improve collaborative working. The Government will outline its approach to future charters in its upcoming Fraud Strategy.

Disrupting and Preventing Fraud 1.3

Background

The 'failure to prevent' offence for bribery has had success in driving better corporate behaviours. A similar offence for failure to prevent fraud being perpetrated using a company's platforms would not only aid prosecution for these failures but focus private sector effort on designing fraud out of companies' systems. (Page 41, Paragraph 37)

Recommendation

A failure to prevent fraud offence should be introduced to hold companies to account for fraud occurring on their systems and encourage better corporate behaviours. (Page 41, Paragraph 38)

Government Response

The Government recognises that the current law on Corporate Criminal Liability does not adequately hold organisations and their senior persons to account for offences committed by the corporation and their associated persons.

In November 2020, the Government asked the Law Commission to do a thorough examination of the issue and present options for reform. This review was published in June 2022.

We are working in collaboration with colleagues across Government to consider the Law Commission's paper and determine a case for strengthening the law on corporate criminal liability, including the creation of an offence for failure to prevent fraud.

Similarly, the Online Safety Bill will, for the first time, create a duty on social media and search engine companies to put into place systems and processes to prevent fraud on their platforms. Ofcom will have extensive powers to enforce this duty, including significant fines and business disruption.

Disrupting and Preventing Fraud 1.4

Background

We are concerned to hear that there is a perception that legislation such as GDPR is preventing the sharing of information and intelligence across sectors where frauds were suspected. Data-sharing laws should not restrict the sharing of information for law enforcement purposes, or where this information could prevent a fraudster being able to move to a new bank or platform to continue their crimes. (Page 41, Paragraph 39)

Recommendation

The Government should provide an update of its review of the legislation in respect of the sharing of data with a Specified Anti-Fraud Organisation. The Government should also look more broadly at the operation of data-sharing legislation with regard to the tackling of fraud and bring forward proposals to ensure data can be shared for the purposes of combatting fraud as soon as possible. (Page 41, Paragraph 40)

Government Response

Sharing data is an important way to identify and disrupt fraudsters from exploiting platforms, services and people to commit their crimes. The Government is clear that this should be a priority for companies and organisations and encourages efforts in this space.

The Government is taking two important steps to support information sharing to prevent economic crime.

Firstly, GDPR establishes the prevention of fraud as a legitimate interest for sharing information. The DCMS-led Data Protection and Digital Information Bill will make it easier for businesses to share information under GDPR for the purposes of preventing economic crime, including fraud, by providing greater assurance around the lawful foundation a business has for sharing data.

Secondly, Reforms in the Economic Crime and Corporate Transparency Bill will also enable businesses, in certain situations, to share information more easily for the purposes of preventing, investigating or detecting economic crime by disapplying civil liability for breaches of confidentiality for firms who share information to combat economic crime. The Government continues to consider the appropriate next steps for the Specified Anti-Fraud Organisation regime.

Disrupting and Preventing Fraud 1.5

Background

Key to the prevention of fraud is increasing public awareness of these crimes and the steps people can take to avoid being victimised. Although campaigns are currently run by the Financial Conduct Authority and its partners, these do not have the level of resources required to proliferate messages about fraud and fraud prevention among the general public. (Page 42, Paragraph 42)

Recommendation

The Government should plan a national awareness campaign as part of the new Fraud Action Plan, to raise public awareness of fraud and the personal actions people can take to reduce their chances of falling victim to such crimes. (Page 42, Paragraph 43)

Government Response

The Government recognises the importance of raising public awareness on fraud, which will form a key part of our forthcoming fraud strategy. One of best ways to safeguard the public is to ensure people are well-informed about the threat and how to protect themselves.

That is why we have established a new public engagement team at the NECC/NCA to drive work across the public and private sectors to coordinate anti-fraud communications, analyse what is most effective, and create consistent messages for the public.

There are numerous existing campaigns that deliver fraud messages, including National Cyber Security Centre's Cyber Aware, FCA's ScamSmart, UK Finance run Take 5 To Stop Fraud, and others run by voluntary and private sector organisations. Action Fraud also conduct regular awareness raising campaigns. We continue to support partners to ensure these communications campaigns are well coordinated, clear and empower the public.