Communications Crime Strategy Group – Written evidence (FDF0063)

The House of Lords has appointed a committee to consider the impact of the Fraud Act 2006 and digital fraud. This submission from the Communications Crime Strategy Group (CCSG) has been prepared for the Committee as an industry input and has not previously been published.

Understanding Fraud Impact in the UK

Office of National Statistics data[1] show that, while most types of crime have been in decline since the mid-1990s, fraud and computer misuse have been growing. Reasons for the increase in fraud in the UK relate to the exploitation by fraudsters of a combination of global technology developments, public policy, and historically low prioritization of fraud by law enforcement.

Communications providers believe better understanding of frauds' causes, impact and potential interventions is needed. This is critical in terms of allocating state and private sector resources and making effective progress in protecting the UK public and economy from fraud.

In July 2021 Which carried out an analysis of categories of fraud reported to Action Fraud – the UK's national fraud reporting service. Which's analysis used Action Fraud data to derive total and average costs of reported frauds by category[2]. See Table 1.

Table 1: Fraud losses by total and individual reported cost

High total reported cost to victims

Fraud Type	Number of Reports	Total Cost	Average Cost
Investment fraud	20,989	£535,139,700	£25,496
Cheque, card, online banking fraud	27,773	£183,900,000	£6,622
Retail/consumer fraud	29,466	£152,700,000	£5,182
Mandate fraud	4,681	£145,700,000	£31,126
Dating scams	7,754	£73,900,000	£9,531
Online shopping & auction fraud	103,254	£69,600,000	£674
Advance fee fraud	38,844	£52,239,600	£1,345
Fraud recovery	2,096	£30,200,000	£14,408
Computer fixing fraud	18,811	£22,100,000	£1,175
Door-to-door fraud	4,373	£21,000,000	£4,802
Fake loan fraud	2,782	£4,100,000	£1,474
Ticket fraud	2,104	£2,100,000	£998
Phone fraud	5,073	£1,500,000	£296

High cost to individual victims

Source: https://www.which.co.uk/news/2021/07/scams -rocket-by-33-during-pandemic/

Investment fraud was the highest fraud category by total reported cost, estimated by Which at **£535M p.a.**. Other high total reported fraud categories were: cheque, card & online banking fraud, retail / consumer fraud and mandate fraud each reported to have cost over **£145M p.a**..

---

1 Source: Crime Survey of England and Wales – September 2021

2 https://www.which.co.uk/news/2021/07/scams-rocket-by-33-during-pandemic/

Average per fraud costs reported by mandate and investment fraud victims were **£31k** and **£25k** respectively. Recovery fraud was reported to cost **£14k** per fraud while dating fraud cost **£9k.** Cheque, card & online banking fraud and retail/consumer reports averaged **£5k** per fraud.

Which noted one third of reports to Action Fraud were uncategorised and that the ONS estimated there were more than four million incidents of fraud in 2020, with only **some 10% of offences** reported to Action Fraud. Inclusion of NI & Scotland data will also increase total fraud impact.

CCSG members believe that an effective anti-fraud strategy aimed at protecting UK citizens and consumers should prioritize action against fraud which cause large total losses to the public and economy and / or large losses to individual victims. See summary of fraud losses in Table 2.

Table 2: Fraud which cause large total losses to the public and / or to individual victims

Large total losses to the public p.a.	**Large losses to individual victims**
➢ Investment fraud (£535M); ➢ Cheque, card and online banking fraud (£184M); ➢ Retail/consumer fraud (£153M); ➢ Mandate fraud (£146M).	➢ Mandate fraud (£31k); ➢ Investment fraud (£25k); ➢ Recovery fraud (£14k); ➢ Dating (£10k); ➢ Cheque, card & online banking fraud (£7k); ➢ Retail/consumer fraud (£5k).

Source: CCSG, based on Which analysis of Action Fraud data

Crime statistics from the Home Office and ONS might improve materially on Which's analysis. There is also scope for discussion of the fraud categories to be considered *"large"* either overall or due to the impact on individual victims. This financial analysis also does not include cases of repeated fraud, affordability or emotional impact on victims: these are clearly relevant for prioritization.

Finally, these reported numbers do not capture the impact to the economy of very large / serious frauds, of frauds against the State including during the recent Covid-19 pandemic, or against businesses such as communications providers. Frauds against the State have been widely reported to create significant losses for the UK and are important in national anti-fraud prioritization.

Looking forward we believe consumer targets of fraud will be mainly unchanged in the near future. These will be in richer countries and segments. Investment fraud, for example, is likely to be a continuing feature. Other fraud types, such as recovery or dating fraud, may be more amenable to suppression through countermeasures and law enforcement action, if they are prioritized. Newer fraud types, such as fraud related to multiplayer on-line gaming and new interactive services, will also become more prevalent. Fraud will be increasingly international in origin and reach.

Government, law enforcement and the private sector should prioritize action against fraud types which create large losses to the public and economy overall and / or large losses to individuals.

What action should follow identification of high-impact fraud types?

Action by Government, law enforcement and the private sector should be prioritized for impact, based on robust analysis and understanding of how high impact frauds occur. This requires systematic analysis of how frauds come to the victim's attention (the in-bound route), consumer / fraudster interaction and how money is extracted by the fraudster (the financial return path).

For each priority fraud type communications providers identify the need for:

- action by the private sector (and by the State where it has proved vulnerable) to harden in-bound routes and financial return paths used by fraudsters, where possible;
- education of customers and staff in fraud awareness including *"in the minute"* responses which will make interactions with fraudsters more resistant to fraud; and
- allocation of law enforcement and other State resources to combat priority fraud types by identifying, pursuing and prosecuting those responsible for significant / repeated fraud incidence in the UK and suitable disruptive and / or deterrence action internationally.

In our sector, the Communications Fraud Charter sets out actions agreed through discussion with Government and other stakeholders as areas where action is being prioritized. With two exceptions these focus on private sector commitments. See Table 3 with exceptions in bold.

Table 3: Actions under the Communications Fraud Sector Charter

Communications Sector Fraud Charter	
Action (1)	Work to identify and prevent scam calls
Action (2)	A co-ordinated approach to tackle smishing
Action (3)	Use of Dynamic Direct Debit to tackle identity theft […]
Action (4)	Use of real-time checking to tackle SIM swap and Mobile Number Porting fraud
Action (5)	Sector information sharing
Action (6)	Systematic sector analysis of shared fraud information and other intelligence
Action (7)	**Engagement by law enforcement to investigate significant / repeated fraud […]**
Action (8)	Improve support given to victims of communications fraud
Action	**Increase fraud awareness**

(9)	

Source: Communications Fraud Sector Charter

The National Economic Crime Centre and City of London Police have engaged with communications providers intelligence leads on significant / repeated fraud (Action 7). The National Crime Agency is investigating approaches and actions by state and private sector to increase fraud awareness (Action 9) including scope for improved coordination of anti-fraud messaging to support awareness.

However, a key issue which remains to be addressed, and which is critical for an effective anti-fraud strategy, is the allocation and management of law enforcement and supporting resources to identify, pursue and prosecute those responsible for significant / repeated fraud incidence in the UK and suitable disruptive and / or deterrence action internationally.

Allocation and management of law enforcement resources

In the Autumn Budget and Spending Review 2021 the Treasury confirmed support for a Government commitment to the recruitment of an additional 20,000 police officers by 2023. It also proposed to allocate an additional £32M from 2022-23 to 2024-25 to tackle money laundering and fraud. There will also be increases in Serious Fraud Office funding into serious fraud, bribery and corruption[3].

However, there remains a substantial mismatch between the impact of fraud on citizens and the UK economy and the allocation of law enforcement effort to fraud. The impact of fraud is substantially greater than the proportion of law enforcement resources dedicated to combat it.

As Graeme Biggar, now Head of the National Crime Agency, commented to the Treasury Committee in January 2021[4]:

> *"In the UK, we do not place the highest priority on fraud across law enforcement and policing. […] in the CSEW, it accounted for about a third of the crime that is reported. It is a lot less in reports that actually get to the police—about 12%—which I can explain in a bit. [However] Only about 1% or less of police resources and personnel are devoted to fraud".*

Communications providers recognize there are a wide range of UK law and order priorities, but we believe more needs to be done by law enforcement to respond effectively to the changing nature of fraud and how resources should be best applied to combat it. We propose that law enforcement and supporting resources to identify, pursue and prosecute fraudsters should reflect fraud's impact when considered as equivalent to other forms of crime against property.

Law enforcement effort in dealing with fraud should reflect its impact as a crime against property. Resourcing should be equivalent with effort to combat other forms of property crime.

---

[3] https//assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1029974/Budget_AB2021_Web_Accessible.pdf

[4] Treasury Committee Oral evidence: Economic crime, HC 917 Monday 25 January 2021

How should law enforcement be organized to combat fraud?

We advocate that the law enforcement response to fraud be organized strategically to combat high-impact fraud types. In particular, fraud officers and supporting civilian staff should be organized in specialist units responsible for combating specific fraud types or combinations of related fraud types where they are identified and agreed to be national policing priorities.

At present law enforcement uses a mix of specialist and general law enforcement resources to combat fraud. Territorial police forces, including Regional Organized Crime Units (ROCUs), are involved where fraud victims or suspects are linked to geographic regions of police operation. We understand that ROCU resources to act against fraud are now being strengthened. However, in many cases there is no link between the range and scale of fraudsters' operation and territorial or regional police operations. This, we argue, is particularly the case with more significant and repeated frauds against consumers and businesses which exploit communications services.

We recognize that organizations such as the National Economic Crime Centre have the capability to create flexible, specialist *"cells"* to address specific law enforcement priorities. It has recently used this mechanism to increase its understanding of bulk scam calls and SMS. We also note that the more significant the fraud or economic crime type, the more likely there already will be a specialized unit addressing this fraud type, including the Serious Fraud Office itself.

Finally, we recognize that the national fraud policing strategy agreed by the National Police Chiefs' Council in October 2019 identified the need for new structures, better co-ordination and increased fraud resources in ROCUs and for the City of London's Police role as national lead force for fraud.

We argue that these law enforcement reforms are the right ones to be more effective in combatting fraud, but that UK law enforcement **has not gone far enough** in its re-organization to effectively combat fraud effectively. Police anti-fraud structures should:

- comprise specialized units, commanded by officers with significant fraud experience and containing officers and support staff with responsibility for combating specific, priority fraud types or combinations of related fraud types;
- have geographical responsibility and range reflecting the location and range of suspected criminals responsible for priority fraud types as well as location(s) of their victims; and
- be tasked with the identification, pursuit and prosecution (in the UK) or disruption (internationally) of suspects who repeatedly and successfully carry out priority fraud types.

We do not advocate either a centralized fraud service or that each individual priority fraud type be allocated to a separate unit. Our proposal is simply that law enforcement's anti-fraud activities be organized specifically to address priority frauds, taking into account the fraudsters' mode and range of operation. Our experience is that greater fraud unit specialization develops policing skills, knowledge and capabilities and will support more effective action against these crimes.

Returning again to Mr Biggar's comments to the Treasury Committee[5]:

> *"Fraud does not happen in the volume that it happens unless it is done in quite a sophisticated way by organised groups, so we need to get that understanding and identify those groups. [and] to pursue those felons in a much more top-down, targeted way. […] better to try to identify groups that are creating the most harm and go after them."*

UK law enforcement anti-fraud activities should be organized strategically to address priority fraud types based on fraudsters' mode and range of operation.

Where and how should intervention take place to reduce the impact of priority frauds?

Communications providers identify three components in the process of defrauding customers:

- the **inbound route**: how a fraud comes to the victim's attention;
- **customer / fraudster interaction** / social engineering of the customer; and
- the **financial return path**: how money is extracted by the fraudster.

What should be done will depend on the nature of the priority fraud type being addressed and which part of the fraud: in-bound route, customer interaction or financial return path is targeted. Fraud types with either bulk scam calls or SMS as routes require responses as shown in Table 4.

Table 4: Illustration of in-bound routes, interactions and financial return paths for certain fraud types

Inbound route	**Interaction / social engineering of consumer**	**Financial return path**
Bulk scam calls Bulk scam SMS	Press #1 to talk to an agent Go to web-site / click URL	Bank payment Bank or other payment
Response	**Response**	**Response (e.g.)**
Fraud charter Actions 1 & 2 including technical measures to address bulk scam calls and SMS. Awareness raising	Awareness raising, including work by the Economic Crime Strategic Communications initiative.	Payment monitoring by banks / financial institutions Awareness raising Action against money mules

Law enforcement identification, pursuit and prosecution of fraudsters make up a fourth component.

Bulk scam calls and SMS have been identified as priorities under Actions 1 and 2 of the Communications Sector Fraud Charter[6]. Communications providers are

[5] Treasury Committee Oral evidence: Economic crime, HC 917 Monday 25 January 2021

now using a range of techniques including filtering / blocking to try to identify and prevent these frauds reaching customers. This could, in certain cases, require **substantially more** activity by telecoms providers – the mid-2021 'flu-bot attacks provide an example where further intrusive measures were required to identify and isolate customers' mobile devices which were sending out bulk SMS.

In supporting formation of its Bulk Telephony Cell, the NECC used an Ofcom estimate of numbers of scam texts / calls received by the public during summer 2021. However, the NECC admitted the*: "National Fraud Investigation Bureau (NFIB) have challenges reliably estimating how much reported fraud is telephony-enabled".* It seems hard to direct private sector or law enforcement resources effectively unless there is better understanding of inbound fraud routes.

As the NFIB implies, evidence quantifying inbound routes used in priority fraud types is hazy. Nevertheless, we suspect a high proportion of victims reporting a fraud, can describe the inbound route if asked and certainly enough to inform effective prioritization and response.

For the communications sector we recognize bulk scam calls and SMS are routes for fraud and we are taking action to harden these services technically. Looking forward we anticipate that, where a message can analysed before delivery, this will become the norm. Caller identification can also be strengthened to combat deceptive origination. However, it will still be possible to call and message globally with individual calls and messages essentially free to originate, including by fraudsters.

Police should develop a robust view of inbound routes associated with priority fraud types to inform effective action and to support customer awareness interventions. Research, including interviews with victims of priority fraud types to understand their experiences, is fundamental.

What about other forms of fraud?

Accepting that effectiveness and efficiency justified action with respect to priority fraud types what should be done in response to other forms of fraud? If law enforcement creates specialist units to address the top 6 fraud categories identified by Which it will be addressing some 80% of classifiable fraud reported to Action Fraud in the period covered.

But what about the other 20%?

Avoiding clichés about the 80/20 rule, communications providers would argue that it is invidious for consumers and the UK economy that **any** area of significant economic crime be left unpoliced. There is a need to combine strategic fraud prioritization with providing a minimum level of deterrent to avoid fraudsters simply migrating from policed to un-policed fraud types.

In Which's analysis phone fraud was classified as 13 out of 13 types of fraud identified with a total cost of £1.5 M to consumers and an average cost of £296. See Table 5 below.

Table 5: Phone fraud

[6] https://www.gov.uk/government/publications/joint-fraud-taskforce-telecommunications-charter

Fraud Type	Number of Reports	Total Cost	Average Cost
Phone fraud	5,073	£1,500,000	£296

Source: https://www.which.co.uk/news/2021/07/scams-rocket-by-33-during-pandemic/

Communications providers are not clear which frauds fall into the category of phone fraud. The impact of frauds such as 1-Ring or Wangeri calls would be low in relation to £300. On the other hand, handset fraud might now commonly approach £1,000 per handset. We take from this that £300 is an average of a basket of different fraud types categorized together under phone fraud.

Our response would be that where there is evidence of significant or repeated fraud in non-priority categories the police should seek to address this with a priority reflecting other crime against property and the quality of the evidence they have to hand from victims' or other reports or are reasonably able to gather.

Again, the complement to effective prioritization by fraud type is to ensure that other areas are not simply left un-policed.

CCSG – 26 April 22

Annex 1: Telecommunications Fraud Sector Charter – Implementation – 16 March 2022

Under the Telecommunications Fraud Sector Charter[7] signatory telecommunications providers[8] agreed to report to HMG and other stakeholders on our activities in support of the Charter at 6 months, 1 year and 2 years.

Timing of this report is 5 months after formal Charter launch on 21 October 2021.

For this initial Charter update signatories can report that activity has begun on all Charter Actions. Administratively signatories have appointed Action Leads for all Actions and a CCSG Member has been identified to provide an escalation route for each Action. Action Leads share progress monthly.

In terms of Action progress, by which we mean progress on agreement on and/or meaningful implementation of Actions, we have self-assessed our activity on each Action to date as being **Ahead**, **On Track** or **Behind** the timetables foreseen in the Charter. See our summary below:

Actions which we believe are currently **Ahead** of anticipated progress:

Action (2) A co-ordinated attempt to tackle smishing	Providers have applied additional technical controls on bulk SMS and financial controls on SIM use. 3 out of 4 UK mobile network providers have implemented SMS network filters.
Action (4) Use of real-time checking to tackle SIM swap and MNP fraud	GSMA's Mobile Connect Account Takeover Protection API is now available from all Charter signatories.

Actions which we believe are currently **On Track** of anticipated progress include:

Action (1) - Work to identify and prevent scam calls	Implementation of certain controls on bulk scam calls by providers. Ofcom has published consultation proposals on CLI reform and other provisions designed to reduce number *"spoofing".*
Action (3) Use of Dynamic Direct Debit to tackle identity theft and subscription fraud	VF UK and Barclays are leads for the cross-industry DDD pilot. A statement of requirements has been agreed between the two lead companies.
Action (5) Sector	CCSG Fraud leads have agreed a Statement of Requirements

[7] See: https://www.gov.uk/government/publications/joint-fraud-taskforce-telecommunications-charter

[8] Signatory providers are: BT EE, Sky Mobile, Tesco Mobile, Three UK, Virgin Mobile 02 and Vodafone UK.

information sharing	of data to be shared. We have also produced an initial Data Protection Impact Assessment.
Action (6) Systematic sector analysis of shared fraud and other intelligence	Providers are developing intelligence on significant / repeated telecommunications frauds affecting customers and firms. Two new intel sub-groups are working on specific significant / repeated fraud types.
Action (7) Engagement by law enforcement to investigate significant / repeated fraud	CoLP and NECC have identified points of contact for providers. CCSG Members participated in a law enforcement / industry / other stakeholder Cell on Bulk Telephony scams convened by the NECC. This is now to be taken forward as a focused collaborative group to develop quality intelligence leads. Providers have joined the NECC threat group and a CCSG representative has been invited to join the NECC Operational Board. NCSC SoR on 7726 to be taken forward under Action 2.
Action (9) Increase fraud awareness	NCA has commissioned research on consumer fraud experience and messaging which has been shared with stakeholders including telecommunications providers.

Action which we believe is **Behind** anticipated progress:

Action (8) Improve support given to victims of telecommunications fraud	Development of an agenda for victim support group discussion. Initial invitation to participate has been extended to victim support groups.

Implementation risks and challenges

For three actions information sharing depends on agreeing a series of documents to support CCSG signatories' data protection obligations. Issues have arisen with coordination, resourcing and agreement on the approaches needed to provide a consistent model based on internal resources.

We now propose to outsource this process and to develop a similar model of documentation customized for each data sharing process.

We have not yet engaged with victim support organizations as provided for under Action 8. We have, however, discussed an engagement model internally and fraud customer care process which we plan to support this engagement.

CCSG - 17/03/22

Annex 2: Specific questions from the Committee's Call For Evidence

The House Of Lords Enquiry invited answers to the following questions in its Call for Evidence:

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?

The considerable recent growth in digital and on-line fraud using communications services reflects a combination of global technology development and sector policy supported by UK and other Governments.

Technology has driven down communications costs, notably, international communications costs reflecting the widespread deployment of high-capacity fibre-optic cables. At the same time fixed and mobile high-speed digital services are now widely available, radically changing the nature of communications consumption, which is now dominated by broadband access. Globally, IT capabilities, the development of the Internet and the use of on-line platforms have all grown hugely and have facilitated development of bulk / automated fraud using readily available PC technology:

> *"The technology to do it is cheap. We actioned a search warrant on a guy we'd located who had been making thousands, if not millions, of calls. We knocked on the door thinking, here we go, and the guy's basically been sitting there in his underpants with a laptop, eating KFC in a small service office. He was just pumping out this stuff through his laptop."*
>
> Andy Curry – Head of Investigations, Information Commissioners Office[9]

Governments internationally have acted to encourage competition in communications services which has radically changed industry commercial models: *"bringing prices into line with costs".* Where competition has not been viewed as effective, sector regulation has been used to drive down prices, notably for voice call and text message termination What this means for consumers and businesses is that communications service access prices are generally higher while usage prices including calls and messages purchased in bundles are very much lower.

Fibre-optic transmission, the growth of the Internet and regulation of call and message termination means that the revenues and commercial focus of UK communications providers is firmly on retail customers. To be profitable in the current UK communications market means that providers must satisfy retail customers with our services, including that these are not polluted by scams. Views that communications providers are incentivized commercially to deliver bulk inbound voice and messaging scams are, frankly, not correct.

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?

The growth of fraud reflects an open, international communications market model which has been encouraged by policy makers keen to support

[9] https://www.theguardian.com/lifeandstyle/2022/mar/18/why-do-i-get-so-many-nuisance-calls-ask-expert

international and global trade. A key challenge now facing policy makers and the sector is the evidence that this model also supports the unwelcome activity of mass fraud against consumers and industry in wealthier sectors and nations.

Managing future fraud risks will require a combination of management of UK-based risks by providers and law enforcement and action against international risks by limiting access to consumers and industry where this is practical or taking other forms of disruptive action where it is not.

We believe consumer targets of fraud will be mainly unchanged over the next 5 to 10 years and will target richer countries and segments. Investment fraud, for example, is likely to be a continuing feature over a 5 to 10-year view. Fraud will continue to be international in its origin and reach.

Other high impact fraud types, such as recovery or dating fraud, may be more amenable to suppression through specific countermeasures such as messaging moderation and / or targeted law enforcement action, if they are prioritized. Newer fraud types, such as fraud related to multiplayer on-line gaming and other interactive services, will become more prevalent. Again, the deployment of gaming platforms of messaging moderation should act to control these risks.

3. Is fraud and its victims treated as a priority? If not, what are the reasons for this. The Committee is particularly interested in responses that can explain any barriers preventing effective counter-fraud cooperation within Government, law enforcement, the public sector and the private sector.

It is commonly recognized that the allocation of law enforcement resources to fraud is low compared to the level of fraud overall and to the impact of fraud on victims.

Communications providers recognize there are a wide range of UK law and order priorities, but we believe more needs to be done by law enforcement to respond effectively to the changing nature of fraud and how resources should be best applied to combat it.

In particular, law enforcement and supporting resources to identify, pursue and prosecute fraudsters should reflect fraud's impact when considered as equivalent to other forms of crime against property.

4. What is the role of international actors in the UK's fraud landscape? What are the barriers to tackling borderless fraud?

As our answer to Question 1 suggests, fraud affecting UK consumers and businesses may be international in nature. Low prices of international communications and IT make the origination of frauds as easy from Bangalore as Brighton.

Responses at a national level should, however, remain a first step – as many frauds are committed from the UK and most involve a UK financial return path.

International action with partner revenue and police services to disrupt frauds is also required.

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?

We advocate that the law enforcement response to fraud be organized strategically to combat high-impact fraud types. In particular, fraud officers and supporting civilian staff should be organized in specialist units responsible for combating specific fraud types or combinations of related frauds where they are identified and agreed to be national policing priorities.

We argue that UK law enforcement **has not gone far enough** in its re-organization to effectively combat fraud effectively. Police anti-fraud structures should:

- comprise specialized units, commanded by officers with significant fraud experience and containing officers and support staff with responsibility for combating specific, priority fraud types or combinations of fraud types;
- have geographical responsibility and range reflecting the location and range of suspected criminals responsible for priority fraud types as well as location(s) of their victims; and
- be tasked with the identification, pursuit and prosecution (in the UK) or disruption (internationally) of suspects who repeatedly and successfully carry out priority fraud types.

We do not advocate either a centralized fraud service or that each individual priority fraud type be allocated to a separate unit. Our proposal is simply that law enforcement's anti-fraud activities be organized specifically to address priority fraud types, taking into account fraudsters' mode and range of operation. Our experience is that greater fraud unit specialization develops policing skills, knowledge and capabilities and will support more effective action against these crimes.

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.

We are not in a position to comment on the activities of the SFO of the CPS. Resources in the CPS to prosecute fraud should reflect the resources applied by law enforcement to detect, pursue and prepare a case against fraudsters so that the system operates without bottlenecks.

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?

One aspect of the wider response to fraud can be the argument that someone else should do more. Better, we believe, to think about the steps in a fraud and be clear about who – industry, government, law enforcement is responsible for action in each case.

We see frauds as consisting of three steps:

- fraud in-bound route;
- customer / fraudster interaction; and

- financial return path.

Communications providers identify the need for:

- action by the private sector including our companies (and the State where it has proved vulnerable) to harden fraud routes and financial return paths where possible;
- education of staff and customers in fraud awareness and responses which will make their interaction with fraudsters more resistant to fraud; and
- allocation of law enforcement and other state resources to combat priority fraud types and to pursue the fraudsters responsible.

Bulk scam calls and SMS have been identified as priorities under Actions 1 and 2 of the Communications Fraud Charter and these are our priorities for action. Providers are now using a range of techniques including monitoring, filtering and blocking to try to identify and prevent frauds using these routes reaching customers.

In terms of *"responsibilities"* we recognize that we have a responsibility for seeking to manage the routes such as bulk voice calls and SMS where these lead to priority fraud types. However, it is also important to understand what can realistically be done by different actors. An example is to understand that while SMS content can be examined for potential fraud before message delivery, the same approach cannot be used for voice call content.

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?

Data Privacy regulation does not limit data sharing, but the processes to agree that sharing can be done under DP legislation / regulation are complex. For the three areas CCSG members are working on under the Sector Fraud Charter we anticipate that each will require the following documentation for direct sharing between providers:

- an agreed description for each data sharing area, setting our objectives / approach;
- a Data Protection Impact Assessment (DPIA);
- a Legal Impact Assessment (LIA);
- a Data Sharing Agreement (DSA); and
- a technical annex to the DSA explaining how the sharing will actually to take place.

In addition, if sharing is to take place via a third party such as Cifas, the UK anti-fraud organization, we will need additional data protection and contractual documentation between providers and Cifas to support this.

To support the 3 areas of data sharing proposed under the Communications Sector Charter we anticipate some 20 documents will need to be prepared and agreed between six or more participating providers representing considerable effort and the consumption of legal resource.

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?

The National Crime Agency is currently leading a review of the messaging to consumers on fraud risks and this should be considered by the House of Lords in its work.

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?

We do not have any comments on the impact of the Fraud Act 2006.

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? Answers may refer to existing mechanisms such as increasing the scope and powers of regulators. You may refer to any legislation and are not limited to the Fraud Act 2006

We do not have any comments on legislative effectiveness.

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

We do not have any comments on the current system for prosecuting fraudsters. The prior activity of ensuring there is effective pursuit of fraudsters is the key area for improvement.

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? Respondents may choose to refer to penalties imposed by the judicial system or by specific sectors.

We do not have any comments on the current penalties for fraudsters. The prior activity of ensuring there is effective pursuit of fraudsters is the key area for improvement.

Best Practice

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

We do not have any comments on this question.

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

Re-organization of policing is key to the more effective combatting of fraud.

We believe UK law enforcement **has not gone far enough** in its re-organization to effectively combat fraud effectively. Police anti-fraud structures should:

- comprise specialized units, commanded by officers with significant fraud experience and containing officers and support staff with responsibility for combating specific, priority fraud types or combinations of related fraud types;

- have geographical responsibility and range reflecting the location and range of suspected criminals responsible for priority fraud types as well as location(s) of their victims; and
- be tasked with the identification, pursuit and prosecution (in the UK) or disruption (internationally) of suspects who repeatedly and successfully carry out priority fraud types.

About the Communications Crime Strategy Group

The Communications Crime Security Group (CCSG) is a forum for crime and security leaders from UK communication providers. Its role is to:

- Set the communications industry's strategic direction on crime reduction;
- Influence the national crime-reduction agenda; and
- Ensure appropriate resources are directed to priority areas.

The CCSG aims to be the *"crime and security"* voice for the communications sector, sharing information and ideas that reduce crime, improve security and build customer trust.

It addresses shared priorities by establishing sub-groups of Members' staff with management responsibility for relevant issues and by acting in partnership with active third-party organizations.

Sub-groups are empowered by the CCSG to share Member information and ideas to reduce the impact of criminal activity, improve Member security and protect customers. Information sharing takes place in a manner consistent with UK Data Privacy and Competition Law and regulation.

CCSG priority areas for 2021 are:

- **Fraud**: technical measures to reduce scam calls, scam SMS and other fraud risks combined with work to improve intelligence sharing, victim support and fraud awareness agreed under the Communications Sector Fraud Charter with the Home Office / DCMS;
- **Physical network security:** metal theft, equipment theft, arson & sabotage; and
- **Intelligence sharing**: collection, management and dissemination of intelligence.

Where sub-groups or third-party organizations identify a requirement for external lobbying of communications industry stakeholders the CCSG facilitates this by:

- Allocating resources to develop appropriate collateral; and
- Ensuring participation of senior-level executives in the delivery of industry's message.

CCSG Members participate in forum and informal discussions on crime and security with UK Government, notably the Home Office, law enforcement including the National Economic Crime Centre, City of London Police and other forces and entities, with regulators including Ofcom and the Information Commissioner's Office and with organizations supporting victims of crime.

CCSG Member companies are: BT EE; Sky Mobile, Tesco Mobile, Three UK, Virgin Media O2 & Vodafone UK.

27 April 2022