trueCall Ltd – Written evidence (FDF0012)

Introduction & credentials

1.1 trueCall Ltd supply call blocking technology that is specifically designed to protect older and vulnerable people from scam phone calls. trueCall units are distributed by 30 police forces, 120 local authority teams, the National Trading Standards Scam Team, Trading Standards Scotland, Age UK and the National Economic Crime Victim Care Unit. These projects report that trueCall block 95%+ of unwanted calls.

1.2 trueCall projects have been funded by DCMS, BEIS, the Scottish Government, the Welsh Government, the Ministry of Justice in Northern Ireland, Police and Crime Commissioners, Proceeds of Crime Funds, and the National Lottery. We estimate that over the life of these projects they will have prevented 14,121 scams leading to savings of over £80m - this is a payback of 50 times the cost of the projects.

1.3 Data from trueCall units is used by all the major enforcement authorities to investigate fraudulent activity. This includes the police, trading standards, Ofcom, the Information Commissioners Office, the National Fraud Intelligence Bureau (part of Action Fraud), Trading Standards Scotland's intelligence team and the National Trading Standards Scams Team.

1.4 Finally, trueCall technology is built into many of the phones that BT sells, and is also licenced by one of the main UK landline networks. We estimate that 2 million UK homes have been protected by trueCall. trueCall technology is also licenced for AT&T and Motorola phones sold in the USA, France Telcom phones sold in France, Turk Telecom phones sold in Turkey and Telstra phones sold in Australia. Worldwide 5 million homes have been protected by trueCall.

1.5 It is important to protect people from scam phone calls. The telephone is a key enabler for fraud as it is a direct and intimate medium – the fraudster can hear your voice, listen to your concerns and objections and respond to them. They can build up trust more easily than via less personal channels such as email or text. Various reports suggest that up to 50% of fraud starts with a phone call. This includes many frauds that are normally classified as Cyberfraud, but which start with a phone call – for example the 'Microsoft scam' (when scammers call you up and persuade you to load a virus onto your computer).

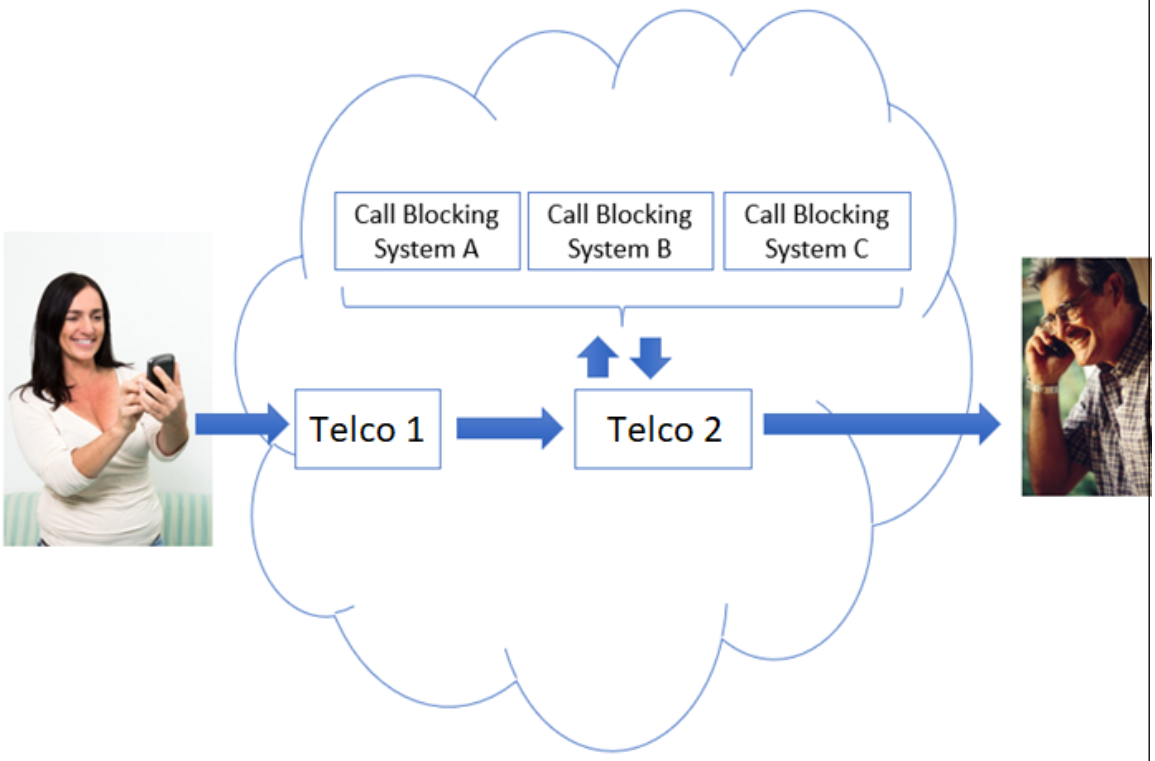
Response to questions

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?
2.1 There are technology solutions available today that can't be rolled out to the people who need them because of the closed nature of telecoms networks. 2.2 There is a range of different call blocking technologies available, and

certain call blocking technologies work better for different people. The most efficient place to mange call blocking is in the telecoms network, and while each individual telco has its own call blocking option, there is currently no open market in call blocking technology*.

2.3 We believe that telcos should be required to expose an open interface so that third party developers can offer their own call blocking services. For example, customers of Telco 1 could then either use Telco1's call blocking service, or they could choose a service from call blocking company A, B or C. The diagram below shows how this would work. When a Telco 1 subscriber calls a Telco 2 subscriber the chosen call blocking solution is used. This approach would work equally well for landline networks and mobile networks.

2.4 This approach would create an open market in call blocking technology, giving consumers choice, and driving price competition and innovation. Telcos have a duty of care to their customers – particularly their vulnerable customers. They should be taking more action to offer consumers the tools they need to block these calls.



* Note that there is an open market on call blocking apps for mobile phones, but apps on mobile phones can only ever have a very limited functionality because mobile operating systems don't give them low-level access to the telephony functions of the phone. Advanced call blocking systems can therefore only be provided as a network service.

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?

5.1 Multiple agencies are involved in work around scams and fraud (see examples below), but there is no common classification of the scam types. For example, a scam associated with solar panels may be classified as a home improvements scam by one agency, a green deal scam by another agency, and an energy scam by another. This makes it very difficult for the agencies to share data, and for a complete picture of the scam situation to be seen.

5.2 We have spoken to many agencies about this who agree that this would be valuable, but none of them individually has the resources to take this on. We suggest that a workgroup is tasked with building a classification model that all agencies can use. A similar model has been built by Stamford University in the USA.

Information Commissioner's Office (ICO)	Which?	The Pensions Regulator
Charity Commission	UK Finance	Phone-paid Services Authority
Telephone Preference Service	Gambling Commission	Solicitor's Regulation Authority
National Trading Standards Scams Team	Action Fraud	Insurance Fraud Bureau
Gambling Commission	OFCOM	Market Research Society
National Trading Standards Intelligence	Fundraising Regulator	Trading Standards Scotland

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.

6.1 We have close relationships with many of the key enforcement agencies involved in tackling fraud so have a good perspective of the problem of telephone fraud. Despite the enormity of the problem they are all struggling with budgets and resources, and this is to do with the 'hidden' nature of fraud. It is often said that while fraud accounts for 40%+ of crime it only gets 1% of police resources. One police officer told us that if they saw a 10% increase in knife crime in their area they would be flooded with resources, but despite a 30% increase in reported fraud over the last year in their region they were getting no additional funding.

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?
9.1 Raising public awareness is key. The 'Friends Against Scams' initiative by the National Trading Standards Scams Team has been hugely effective.

15. Can you suggest one policy recommendation that the Committee should make to the Government?
15.1 Many scammers 'spoof' their phone numbers – send an inauthentic caller-ID with their calls – which allows them to hide their identity. This makes it extremely difficult to identify the scammers, and, if they are based overseas, in taking action against them. However, many call centres use actual UK phone numbers for making their calls. These should be the low hanging fruit – the scammers that can be traced from their phone number and which are located in the UK. 15.2 The problem is that the provision of phone numbers is currently lightly regulated. Ofcom issues blocks of phone numbers to telecoms companies who become the 'range holders' for those numbers. The range holder may then sell on these numbers to end users, or maybe to other telecoms companies who resell the numbers. These resellers may sell numbers to other resellers who may sell them to other resellers. While Ofcom have some control over the range holders, they have no control of the resellers. 15.3 We frequently hear of situations where enforcement authorities see a particular phone number is being used to make scam calls. When they go to the range holder to find out who is operating the number they are met with a refusal to co-operate. 15.4 We propose:

1	When a range holder gets a request for phone numbers they should carry out 'Know Your Customer' (KYC) checks to evaluate the customer - identity checks, Companies House checks, bank detail checks. The range holder should ascertain the type of business and intended use for the numbers. Note that often third parties are used by a fraudster to act as a front, and they themselves have no direct involvement in the business. As per money laundering rules, KYC checks should be carried out at least annually or when there is a material change in the business, i.e change of bank, premises, directors, location or business style.
2	Complaints about numbers should be fed back to the range holder for investigation. This could be done via the agencies that received the complaints – Action Fraud, Ofcom, the Information Commissioner,

	Telephone Preference Service, National Trading Standards Scams Team, etc.
3	Range holders should be obliged to carry out regular checks on the numbers that they have issued: 1. To ensure that the call volume and profile of the calls matches the intended use specified by the customer. Large numbers of short duration calls is a red flag suggesting high volume telemarketing or scams. 2. To ensure that the user of the numbers is compliant with Ofcom's regulation to prevent persistent misuse of the telephone network. 3. To review complaints about the phone numbers from regulators and enforcement authorities, but also from public sources (the Who-Called.co.uk), and commercial organisations such as ourselves [we must declare an interest here]. If the numbers are being misused the range holder should take action, potentially shutting down the number.
4	There should be a requirement on range holders to evidence that they have carried out the appropriate checks. They should provide Ofcom with a quarterly report on the KYC checks they have carried out, the monitoring checks they have carried out, the complaints they have received from the public, their evaluation of the customer and the actions that they have taken. They should make available to Ofcom, on request, full details of the investigations they have carried out including all the evidence they used to reach their conclusion.
5	Range holders should be obliged to respond in timely manner to requests from police, trading standards and other legitimate enforcement authorities for information about numbers in their range. They should be obliged to provide contact details of the number user and call detail records for any number in their range if requested.
6	These regulations should apply to range holders and also to anyone else who buys phone numbers for resale.

15.5 Ofcom are currently consulting on introducing a best practice guide that encourages range holders to carry our Know Your Customer checks. We don't believe that this is enough. It would be too easy for providers to 'look the other way' and ignore clear abuse carried out using the phone numbers that they provide. In our view this should be a regulatory requirement similar to other regulated sectors under Anti Money Laundering regulations.

By requiring range holders to be responsible for Know Your Customer and monitoring checks you introduce jeopardy since the money laundering rules can apply where a company has knowingly enabled a fraudster to operate.

15.6 We acknowledge that our proposals will impose additional costs on the range holders, but the cost to the public from scam phone calls is measured in the billions of pounds a year and it seems to us that it is reasonable that those who supply the numbers and profit from them are made responsible for ensuring that the numbers and services that they sell are being used legitimately.

19 April 2022