BT Group – Written evidence (FDF0067)

Summary

- The scale of fraud in the telecommunications sector - scams generated by phone and SMS is still significant.
- The activity and the trends that we saw during the Pandemic was alarming – both in terms of the scale of fraudulent activity and its targeting of our most vulnerable customers in isolated and difficult situations.
- BT has increased and extended its ongoing programme of investment and innovation to protect its customers. Our business and reputation are dependent on customer trust and security, and it is therefore a top commercial (as well as a moral and ethical) priority to ensure we take protective action wherever possible against fraudsters.
- Digital fraud is a complex cross industry issue. To make progress telecommunication companies need to work with each other, financial institutions, regulatory bodies, Government and law enforcement to reduce the incidence and impact of digital fraud. BT is an active member of multiple initiatives to counter fraud.
- It is critical that network operators and financial institutions, in particular, work together to share best practice and improve security. We have a strong commercial incentive to provide the best possible service and support to the UK's major financial services companies, given that many of them are current or prospective customers.
- Given the complexity, Government has a key role to play in convening interested parties and driving forward coordinated action. Having one department in the lead, with one Minister responsible for all outcomes would bring clarity and enable all stakeholders to work together on agreed priorities. The Telecommunications Sector Fraud Charter and the telecommunications sector involvement with the National Economic Crime Centre is helping to improve coordination.
- Consumer and public education will always be a key part of tackling digital fraud, to empower individuals to guard against fraudulent approaches. Again, co-ordination from Government could improve the impact of existing efforts here.
- The fight against fraud will remain an ongoing battle: fraudsters are increasingly sophisticated in the social engineering of victims to hand over key information using multiple communication channels and we anticipate that as fraud over telecommunications get harder they will turn to other digital technologies such as encyrpted messaging apps to try and commit fraud.
- Our free anti-spam tool launched in July 2021 has blocked more than 120 million scam SMSs and reduced customers' reports of scam SMS by 91% via 7726, and our free BT Call Protect tool used by 4.4 million customers has diverted 366 million scam calls. Work that we have in train and will implement this year is projected to have a similar impact on spoof landline calls from overseas. However, there is more to do, not least in coordinating with law enforcement to bring prosecutions. But together these measures

represent a very significant step forward. It also important that Ofcom lifts the bar so that all network operators implement similar measures.

Legal and law enforcement aspects

- We believe that legislative and regulatory requirements do not present a significant obstacle to fraud risk data sharing, but a Government led process consulting with Ofcom to establish standards and norms would be helpful.
- We do not consider that amendment to the existing Fraud Act offences is required to address online fraud. The main obstacle to tackling modern forms of fraud is resource and international co-operation.
- We would welcome increased and effective cooperation between UK law enforcement agencies and their international counterparts to tackle fraudulent landline calls and prosecute criminals**.**

What BT does to protect its customers from fraud

We have made significant investment and will continue to do so to protect our customers. Our approach / key activities to protect our customers is as follows:

- Securing our fixed and mobile networks against network security /cyber-attacks to protect our customers against fraud/data theft.
- Providing customers with free security and privacy tools including implementing and developing new blocking solutions for our fixed and mobile networks to stop unwanted calls and SMSs.
- Providing customers with advice on how to spot and handle a scam and what to do if they are targeted by scammers.
- Working in partnership with other Communication Providers (CPs), financial institutions, regulatory bodies such as Ofcom, Government and law enforcement to combat this fraudulent activity.

Further details on each of these activities can be found in the Annex.

BT response to Call for evidence questions

Fraud Landscape

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

BT response

1.0 The Telecommunications Fraud Sector Charter outlines the specific fraud risks / reasons for vulnerability in the telecommunications sector which are outlined below:

1.1 Fraud risks directly affecting telecommunications customers

- Scam Calls: Criminals call to obtain personal information, socially engineer and/or defraud the victim. Scam calls are made more realistic by number "spoofing", which makes the call appear to be from a trusted number.
- Smishing: Criminals use SMS/text messages to obtain personal information, socially engineer and/or defraud the victim.

1.2 Fraud risks resulting in wider customer financial fraud

- Identity Theft / Subscription Fraud: Criminals use personal data, which may be illegally obtained, to apply for mobile devices and other credit services in the victim's name. Customers suffer identity theft and telecommunications providers subscription fraud.
- SIM Swap/ Network Divert Fraud: Criminals take over a customer's account by applying for a new SIM or network divert in their name. Criminals use personal data, which may be illegally obtained, and other credentials to pass security checks to access the victim's accounts.
- Mobile Number Porting Fraud: Similar to SIM Swap, a criminal transfers a victim's number to another network to intercept communications intended for the victim to access the victim's accounts.

1.2 Online fraud risks for businesses

The most common types of cybercrime facing businesses, according to the Federation of Small Businesses (FSB) are:

- Phishing: web sites, phone calls and spam emails that appear legitimate, but are scams designed to acquire private data.
- Malware: malicious software installed inadvertently, usually by visiting a malware-infected (but otherwise genuine) website, or by opening an attachment from a phishing email.
- Denial of Service (DOS): a mass orchestrated attack that floods a computer system (often a website) with countless requests for information, rendering it incapable of responding to real users.
- Ransomware: a type of malware that locks users out of a computer system, often by encrypting its data, and threatens deletion until a ransom is paid.

1.3 Further information / research on the most prevalent phone and online scams targeted at individuals was published by Ofcom in October 2021.

1.4 Online scammers have become very sophisticated in the social engineering of victims to hand over key information / personal details and are using multiple communication channels and spoofing well-known companies and organisations. The FCA's Perimeter Report 2020/21 stated that "fraudsters have unprecedentedly cheap access to an online population of consumers who find it difficult to differentiate legitimate offers from fraudulent ones." For businesses particularly SMEs

insufficient staff training along with poorly implemented IT policies make it easy for scammers to commit fraud. For example, small businesses who are using dated versions of Internet Explorer

present security holes for cybercriminals to exploit. Upgrading to the latest version of a browser will block most web phishing attempts and a wide range of other web-based attacks.

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?

BT response

2.0 It is very difficult to predict accurately developments that will impact how fraudsters will commit crime over the next five to ten years. However, as more businesses become digital, fraudsters will also increasingly use new digital techniques in order to commit fraud.

2.1 With regards to economic developments the global economy is seeing an increase in energy/fuel costs, and supply chain delays are increasing the cost of food/ some consumer goods. These increases are putting financial pressure on individuals which may create a need for additional income, at any cost including fraudulent behaviour. Furthermore, people are increasingly investing in cryptocurrencies which will provide criminals with an opportunity to commit fraud.

2.2 It is likely that fraudsters will seek to increasingly use social media or search engines to commit fraud particularly investment fraud as reported by Action Fraud. Therefore, it is welcome that the Government is making changes to the Online Safety Bill to protect people from scam adverts online and consulting on a wider overhaul of how online advertising is regulated in the UK, including proposals to improve transparency and accountability and tackle harmful, fraudulent and misleading adverts. UK Finance[1] has stated that "the current legal and regulatory framework needs to be updated to keep pace with the rapid growth in these online scams. Currently, the tech giants are not properly held accountable for fraudulent content promoted on their platforms. In some cases, these firms are even being paid by the criminals to place scam adverts on their platforms. It cannot be right that online platforms are profiting from these scams, while the rest of society is left to pay the price"

2.3 techUK have established that organisations are under increased consumer pressure to provide a seamless and frictionless user experience, with consumers saying they'll abandon an online transaction if security checks take longer than 30 seconds. That provides fraudsters with opportunities to exploit. To help mitigate the risk of faster/fewer security checks organisations will invest in new identity verification processes such as facial and age recognition technology, and also deploy behavioural biometrics/artificial intelligence to monitor human behavioural patterns and consumer transactions to detect suspect payments.

[1] FRAUD - THE FACTS 2021THE DEFINITIVE OVERVIEW OF PAYMENT INDUSTRY FRAUD

2.4 The rise of encrypted services creates new opportunities for fraudsters, about which telecoms companies can do nothing. Encrypted services are marketed as better protecting the users data from hacking, and this is true for technical attacks seeking to capture valuable information such as bank details. However, if a user is deceived into contact with a fraudster on an encrypted platform such as WhatsApp or Apple's iMessage (the way many Apple phone users message each other) then teclos have no visibility of any aspect of these communications, and the measures discussed in this response are not relevant.

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.

BT response:

3.0 Yes fraud is a priority for BT. We have a BT Group wide team working on it, that meet regularly with Marc Allera, CEO of BT's Consumer business and other members of BT's Executive Committee.

3.1 We have made significant investment and will continue to do so to protect our customers. Our approach / key activities to protect our customers is as follows:

- Securing our fixed and mobile networks against network security /cyber-attacks to protect our customers against fraud/data theft.
- Providing customers with free security and privacy tools including implementing and developing new blocking solutions for our fixed and mobile networks to stop unwanted calls and SMSs.
- Providing customers with guidance on how to spot and handle a scam and what to do in the event they are targeted by scammers. Our call centre colleagues are also trained to help customers who receive scam calls and we have a specialist team to support customers who may have inadvertently given their account details to criminals. We help customers rescue their service and advise them to contact their banks.
- Working in partnership with other CPs, financial institutions, regulatory bodies such as Ofcom, government and law enforcement to combat this fraudulent activity.

3.2 BT is part of the Communication Crime Strategy Group (CCSG) which is made up of a number of CPs whose aim is to tackle fraud across our sector. The CGSG judge that more needs to be done by law enforcement to respond effectively to the changing nature of fraud and how its resources should be best applied to combat it. In particular, police effort in dealing with fraud should reflect fraud's impact when considered as equivalent to other forms of crime against individuals and property. Graeme Biggar, Director General of the National Crime Agency, commented to the Treasury Committee in January 2021 "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 actual 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".

3.3 We recognise that the scale of the problem from telecommunications fraud such as phone and SMS scams is still very significant. We believe more progress can be made through greater coordination within the sector, across other sectors, with law enforcement and various Government agencies. The Treasury Committee Economic Crime Report also highlights that there a large number of agencies responsible for tackling fraud who have different priorities for types of fraud. This can be confusing for not only victims but businesses because this can lead to differing advice and guidance. It is also a barrier to effective counter fraud cooperation. We would agree with the Treasury Committee Economic Crime Report that there should be "a single law enforcement agency with clear responsibilities and objectives."

3.4We agree with the Treasury Committee Economic Crime Report[2] that the low prioritisation of economic crime from many stakeholders, including parts of Government and law enforcement may be because it "does not happen in the street, but often in people's homes. Consumers often, apart from inconvenience, do not suffer directly, since they may be repaid by banks".

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

BT response

4.0A great majority of landline scam calls originate outside the UK so the role of international actors is vital to tackling this type of fraud. We have an investigation specialist based in India who works with industry particularly Microsoft and law enforcement agencies. Securing Indian Police action has recently improved with raids, arrests and confiscation of equipment but more needs to be done. The number of voice scams reported into Action Fraud (and BT) drops significantly when law enforcement activity does take place in India.

4.1A barrier to increased and effective cooperation between UK law enforcement agencies and their international counterparts is having insufficient resource with priority likely to be given to domestic criminal activities which are easier to prosecute. Another barrier is that traditional mutual legal assistance regimes are not designed for the digital age, with processes being slow and too lengthy to facilitate effective cross-border collection of electronic evidence.

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

[2] Treasury Committee Economic Crime Report Feb 2022

the National Fraud Intelligence Bureau, at executing their role as the lead police force for fraud?

BT response

5.0 See paragraph 3.3. The City of London Police play an effective role in tackling fraud but it only has limited resources to deal with the very large problem of fraud. Furthermore, local Police Forces do not have dedicated time and expertise to properly investigate and tackle fraud. In our sector we are also seeing a delay in cases reaching the Courts particularly when suspect(s) plead not guilty. We welcome the Police Uplift Programme which is increasing policing resources across regional organised crime units and also within the City of London Police. We also understand that the City of London Police – Action Fraud - are looking at procuring new IT systems which should improve their ability to tackle fraud.

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.

BT response

6.0 As above.

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?

BT response

7.0 The private sector has a key responsibility to detect, prevent and help their customers when they become victims. As digital fraud is a complex crime perpetrated across multiple industries the private sector should work with each other, financial institutions, regulatory bodies such as Ofcom, Government and law enforcement to reduce the incidence and impact of digital fraud.

7.1 However, addressing fraud will always be an arms race between those of us seeking to prevent it and the perpetrators. As fraud has become difficult to achieve, fraudsters have shifted to social engineering that relies on human fallibility. As industry manages down the risks e.g. preventing large sums of money from easily being transferred online – fraudsters will likely shift back to data hacking to steal money digitally. Likewise, new and unregulated sectors like cryptocurrencies create new opportunities to defraud individuals.

Sadly, it will never be possible to completely protect the public from fraud, though it is possible to greatly reduce the volume of fraud that is initiated, or if initiated goes on to succeed.

7.2 A balance needs to be found between on-going efforts and innovations to prevent and disrupt fraud and other industry investment that is proportionate. The telecommunications sector is a low return industry compared to big tech[3], or banking so we weigh these choices carefully. However, we are also motivated to ensure our customers can be confident using our products and services, so our interests our aligned with our customers in continuing to invest and innovate to combat fraud that originates via our services.

7.3 Within the telecommunication sector there has been a good level of cooperation and information sharing. Examples of where BT and the wider telecommunications sector works together to combat fraud includes:

- BT sits on the National Economic Crime Centre (owned by the National Crime Agency) which is a public and private partnership.
- BT is part of the Communication Crime Strategy Group which is made up of a number of other CPs whose aim is to tackle fraud and criminality across out sector.
- BT is a founding member of Stop Scams UK (SSUK), which works to co-ordinate the efforts of CPs, financial institutions, and law enforcement to detect and prevent scams.
- BT is a signatory to and helped develop the Telecommunications Sector Fraud Charter with other CPs/mobile operators in conjunction with the Home Office, DCMS, Ofcom and other stakeholders. The Charter represents an opportunity for an intensification of coordinated sector and cross-sector action to fight back against fraud.

The Telecommunications Sector Fraud Charter and the telecommunications sector involvement with the National Economic Crime Centre has only been in place for around six months so its success in tackling fraud is still being evaluated but early indication is that it is seeing improved coordination.

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?

BT Response

8.0 In our view legislative and regulatory requirements do not present a significant obstacle to data sharing in this area, given the extent of the threat to the public posed by online fraud. The General Data Protection Regulation

[3] https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/how-telcos-can-succeed-in-launching-new-businesses-beyond-connectivity

provides several lawful bases for processing which may be applicable depending upon the circumstances, most commonly:

- processing is necessary for compliance with a legal obligation to which the controller is subject (UK GDPR Article 6.1 (c));
- processing is necessary for the performance of a task carried out in the public interest (UK GDPR Article 6.1 (e)); and
- processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child (UK GDPR Article 6.1 (f)).

Where there are issues in this area, they tend to involve the question of whether in the specific circumstances of the case, the sharing of personal data is proportionate i.e. adequate and relevant for the purposes of processing.

8.1 Such sharing may also involve processing special category data. Article 9 of the UK GDPR provides the basis on which special category data may be processed, including that:

- processing is necessary for reasons of substantial public interest, on the basis of domestic law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject (UK GDPR Article 9.2 (g))

8.2 The basis for the processing under UK law is provided in the DPA 2018. Section 10(3) of the DPA provides that the requirement above is met if a condition set out in Part 2 of Schedule 1 to the Act applies.

8.3 Part 2 of Schedule 1 requires a data controller processing special category data on the basis of substantial public interest to have in place an appropriate policy document setting out the basis for compliance with data protection requirements. Additionally, paragraph 10 of Schedule 1 provides:

- This condition is met if the processing -
  - is necessary for the purposes of the prevention or detection of an unlawful act,
  - must be carried out without the consent of the data subject so as not to prejudice those purposes, and
  - is necessary for reasons of substantial public interest…

8.4 The obtaining of network information relating to online fraud risk will also usually involve an interception of communications. This can generally be carried out on the basis that the provider has contractual basis for monitoring and blocking, and in some cases passing information to the

relevant public authorities. However sections 45 and 46 of the Investigatory Powers Act, and the Investigatory Powers (Interception by Businesses etc.) Regulations also provide a lawful basis for such monitoring. Section 45 relates to interception by telecommunications providers of communications

on the service which they provide, and section 46 interception by businesses more generally, of communications sent via networks which they control.

8.5 Regulation 3(2) of the Regulations provides that lawful interception of communications by a telecommunications system controller may take place for the prevention or detection of crime. We are required to make reasonable efforts to inform our customers that we may undertake such interception, which we do via our public Privacy Policies. Other provisions under Parts 2 and 3 of the Act may also enable warrants or authorisations to be given to CPs to provide intercepted content or retained communications data to various public authorities, and there are other powers such as a Production Order under Schedule 1 of the Police and Criminal Evidence Act 1984.

8.6 In general, therefore we consider that we have an adequate legal and regulatory basis for data sharing in this area.

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?

BT response

9.0A key element in tackling fraud is to ensure that individuals/customers are provided with the necessary advice and tools to guard against fraud. We believe that our customers are generally well informed about the risks of fraud and how to prevent them but recognise that more can be done, for example promoting the 7726 service for scam text/mobile calls. Furthermore, certain groups of older people may not be well informed because of their personal circumstances such as social isolation, and cognitive impairment. We promote and provide all of our customers with advice and information which covers types of scams, how customers can protect themselves, how to report a scam, the latest scams, and popular links for more advice e.g. Action Fraud. Also, via our BT Skills for Tomorrow and Tech Tips campaigns we provide online videos on how to stay safe online e.g. how to avoid online phishing. Customers without internet access can also call our Nuisance Calls Advice Line (NCAL) on 0800 661 441 for advice and to report nuisance calls. We've also worked with the National Cyber Security Centre on all our security education and advice for customers. Customers can also call our call centre colleagues who are trained to provide advice.

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?

BT response

10.0 BT's main experience is in the area of scam calls, online and online-enabled fraud. To the extent that we are in a position to comment, we note that successful fraud prosecutions are complex and difficult even in the offline world, given the difficulty of proving elements such as dishonesty and knowledge/intent particularly where a defendant may be remote from any loss caused to the victim. These issues are only amplified in the case of international scam calls and online fraud, where the difficulty of tracing perpetrators and the ease and volume of production of fraudulent communications through various different channels tends to make the risk/return analysis more attractive for online criminals.

10.1 We have not seen any specific unintended consequences 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

BT response

11.0 We do not consider that amendment to the existing Fraud Act offences is required to address online fraud. In our view the main obstacle to tackling modern forms of fraud is resource and international co-operation, particularly for "lower level" consumer and SME fraud, which may be of relatively low value in individual cases but has a significant impact and cost across the population as a whole.

11.1 However, additional domestic legislation could assist the reduction of online fraud by criminalising collateral conduct which is closely associated with fraud, but would not necessarily require proof of dishonesty – for example being involved in the distribution of "scam" communications or the hosting or promulgation of "scam" advertising (some of which we understand may be considered in context of the Online Safety Bill). Such legislation could additionally involve an extra-territorial element similar to the "significant link with domestic jurisdiction" required in legislation such as the Computer Misuse Act, to assist prosecution of suspected perpetrators who are not based in the UK.

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

BT response

12.0 To the extent that we are able to comment, we would consider the resources and co-operation required to trace perpetrators, particularly given the international nature of most scam call and online fraud operations, the

proliferation of mass market anonymisation and encryption tools, and the ease of conducting online fraud at scale to be the key barriers to successful prosecution.

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.

BT response

13.0 We are not in a position to respond.

Best Practice

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

BT response

14.0 We would agree with the conclusion in the Treasury Committee Economic Crime Report [4]that there is no "silver bullet" solution …….. it can only work if there is extensive co-ordination at all levels, from Ministers to those on the ground who are enforcing the law". So relentless coordinated efforts from all stakeholders is required to bring about multiple incremental gains which keep pace with and push back against fraudsters. Effective policy intervention also occurs when regulatory/industry proposals are adopted by the whole of industry and not just by the main industry players.

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

BT response

15.0 A great majority of scam calls originate outside the UK so the role of international actors is vital to tackling this type of fraud. We would welcome increased and effective cooperation between UK law enforcement agencies and their international counterparts to tackle this type of fraud and prosecute criminals**.**

ANNEX

What BT does to protect its customers from fraud

[4] Treasury Committee Economic Crime Report

Securing our fixed and mobile networks against network security/cyber attacks

- We have a significant number of employee experts who work to protect our networks from a huge number of cyber-attacks ranging from large scale attacks such as distributed denial-of-service (DDoS) attacks to more targeted attempts to steal customer data such as phishing sites. Our protection involves monitoring external threats and gathering intelligence on evolving cyber techniques, tactics and capabilities. For example, we monitor and manage customer and BT devices around the clock from 16 accredited global security operations centres, and we protect BT from over 125,000 cyber-attacks every month. We also promote good security 'hygiene' and behaviour in our colleagues, through communications, campaigns and training.

Providing customers with free security and privacy tools

- We offer free and easy to use security and privacy tools such as BT Call Protect, which helps stops unwanted calls. BT customers can call 0800 800 150 or visit bt.com/callprotect if they'd like to sign up. They can also go there to see what calls they've received recently – and block them if they want to. Our network experts also monitor nuisance call makers – the worst are added to our Call Protect blacklist and get diverted before they reach customers. BT Call Protect is used by 4.4 million BT customers and has diverted 366 million since launch, averaging at 2.35 million per week in the past few months.
- We also offer BT Web Protect used by 5.2 million BT customers which protects against malicious and harmful websites, and BT Virus Protect which protects against malicious and harmful viruses and spyware, currently being used by 650K BT customers. Furthermore, in July last year we launched EE's new anti-spam filter which helps prevent malicious phishing and scam SMSs being received by customers. More than 120 million SMSs have already been blocked and the anti-spam filter has reduced customers' reports of scam SMS by 91% via 7726. We encourage customers to help us act by texting reports of nuisance SMS messages to 7726. EE and the UK's mobile operators worked together to deploy a tool which collates all the information from the 7726 short code in real time which allows early action to block numbers that are generating spam on their networks.
- Customers can also sign up to BT Privacy, which is a free service to all customers with a 12-month line rental contract. This service lets individuals register with the Telephone Preference Service (tpsonline.org.uk) – a central register where customers can record their preference so they don't get unsolicited sales or marketing calls. This service also comes with free Caller Display, so customers can see the number calling them and decide whether or not to pick up.

Implementing & developing new blocking solutions for our networks to stop unwanted calls and SMSs

- We deploy/block the Ofcom Do Not Originate list on our mobile and Public Switch Telephone Network platforms which are numbers allocated to banks and other financial institutions, but which are never used for outbound customer service calls. While BT will always block the numbers making automated calls once reported into us, fraudsters will always generate new numbers. They'll also use unallocated numbers to try spoof legitimate numbers in order to make themselves look legitimate to their potential victim. BT takes a number of steps to actively counter this by analysing these scam calls and illegal traffic and take the appropriate action where we can. For example, where feasible BT has taken steps to prevent calls from unallocated numbers that Ofcom maintains under the National Telephone Numbering Plan (NTNP). BT is also working closely with other Service Providers to tackle this issue. For example, where we identify a "spoofed number" deliberately making thousands of unnecessary calls, we work with other Service Providers who unintentionally carried these calls into our network (to apply the relevant blocks and stop the calls getting through).
- We are working to implement a solution this summer for our voice platforms to block more calls originating from abroad that use a UK Calling Line Identity (CLI) – the number that appears on your phone telling you who (what number) is calling you.

Providing customers with advice and guidance

- We warn our customers to be on their guard against scams. For example, we promote and provide all of our customers with advice and information which covers types of scams, how customers can protect themselves, how to report a scam, the latest scams, and popular links for more advice (e.g. Action Fraud). Also, via our BT Skills for Tomorrow and Tech Tips campaigns we provide online videos on how to stay safe online e.g. how to avoid online phishing. Customers without internet access can also call our Nuisance Calls Advice Line (NCAL) on 0800 661 441 for advice and to report nuisance calls. Our call centre colleagues are also trained to help customers who receive scam calls and we have a specialist team to support customers who may have inadvertently given their account details to criminals. We help customers rescue their service and advise them to contact their banks.

Working in partnership with others

- As this is an industry-wide issue we are committed to work with all CPs, financial institutions, regulatory bodies such as Ofcom, ICO, government and law enforcement to reduce the incidence and impact of fraud from scammers.
- Since the start of the pandemic we have worked closely with Law Enforcement sharing intelligence resulting in arrests, and convictions, for SMS fraud (known as smishing). We have recruited an investigation specialist based in India who works with industry and law enforcement. BT also sits on the National Economic Crime Centre (owned by the National Crime Agency) public and private partnership, and BT is part of the Communication Crime Strategy Group which is made up of a number of CPs whose aim is to tackle fraud and criminality across out sector.

- BT is a founding member of Stop Scams UK (SSUK), which works to co-ordinate the efforts of CPs, financial institutions, and law enforcement to detect and prevent scams. We have systems in place to notify financial institutions of any suspicious activity, for example regular SIM swaps.

We are a signatory to and helped develop the Telecommunications Sector Fraud Charter with other mobile operators in conjunction with the Home Office, DCMS, Ofcom and other stakeholders. The Charter represents an opportunity for an intensification of coordinated sector and cross-sector action to fight back against fraud.

4 May 2022