Home Office

Government Response to the Consultation "Preventing the use of SIM farms for fraud"

A summary of consultation responses and the way forward

November 2023

CP 978

Government Response to the Consultation “Preventing the use of SIM farms for fraud”

A summary of consultation responses and the way forward

Presented to Parliament
by the Secretary of State for the Home Department by
Command of His Majesty

November 2023

CP 978

This publication is available at www.gov.uk/official-documents.

Any enquiries regarding this publication should be sent to us at **SimFarmConsultation@homeoffice.gov.uk**

ISBN 978-1-5286-4563-8

E03015619 11/23

Printed on paper containing 40% recycled fibre content minimum

Printed in the UK by HH Associates Ltd on behalf of the Controller of His Majesty's Stationery Office

Contents

Ministerial Foreword

As Security Minister, I am committed to stopping fraudsters from making victims of us all. The barrage of scam texts and phone calls we have seen from fraudsters causes emotional distress and financial misery to millions. This is why we set out our commitment to block frauds by reducing the number of scam communications that get through to the public in the Fraud Strategy, published in May this year.

At the same time, we consulted on proposals to ban SIM farms to stop criminals getting hold of and using these devices to scam the British public. The public response to the consultation on this issue is clear: people want to see more protection from fraud and for the Government to take further action to crack down on fraudsters.

Today, I am pleased to be able to publish the Government's response to the consultation, which paves the way for legislation to reduce telecommunications enabled fraud. The response sets out our plans to ban the possession and supply of SIM farms, whilst ensuring that there are adequate protections for legitimate businesses.

The new offence will mean criminals are no longer able to obtain SIM farms and similar technologies to commit fraud. This will give police additional tools to disrupt the vile criminals that target the UK public.

Tom Tugendhat

Rt Hon Tom Tugendhat MBE VR MP
Security Minister

Executive summary

This document sets out the Government’s proposed measures to prevent the use of SIM farms for fraud in the UK. In May 2023, we consulted on a potential ban on SIM farms, defined as devices that can make calls and texts and hold more than 4 SIM cards at one time. We are grateful to those who took time to respond to the consultation.

The Government will bring forward legislation creating a new criminal offence of supplying or possessing a SIM farm subject to defences to allow for legitimate use and where adequate due diligence has been undertaken. The offence will carry a penalty of an unlimited fine.

The Government will also bring forward legislation to allow the extension of this offence to other specified telecommunications devices or articles, where there is a significant risk of them being used for fraud. Any extension of the offence will be subject to a requirement to consult any affected parties to ensure proportionality.

We believe that the new offence will give police additional tools to disrupt criminals and make it more difficult to access and abuse SIM farms and similar technologies for fraud.

Consultation overview

The case for action

As set out in the Government’s Fraud Strategy[1], fraud now accounts for around 40% of all estimated crime in England and Wales. This is exacerbated by the increasing technological sophistication of the tools available to fraudsters, which allow them to target victims at scale.

Short Messaging Service (SMS) messages are a method used by fraudsters to target the UK public. Texts are the most common form, with more than 6 in 10 people reporting that they had received suspicious texts in a three-month period. Reports of suspicious calls are lower but still significant: 21% of respondents reported suspicious live calls to their mobiles and 19% to their landlines[2]. SIM farms are available on popular online marketplaces, at low prices, with limited or no requirement to verify the buyer’s identity. This makes them an easy to access, low-cost option for fraudsters who use them to deceive victims into giving sensitive information such as bank details.

The Government is committed to stopping criminals from exploiting SIM farms to defraud the UK public.

Consultation process

The Home Office consultation “Preventing the use of SIM farms for fraud” was launched on 3 May 2023 and closed on 14 June 2023. It sought views on the definition and potential legitimate uses of SIM farms in light of a potential ban. The consultation also sought views on other technologies used by fraudsters and asked whether the Secretary of State ought to be able to ban other similar equipment in the future. The consultation is available to view at: https://www.gov.uk/Government/consultations/preventing-the-use-of-sim-farmsfor-fraud.

Responses to the consultation support the Government's approach to addressing the issue of SIM farms being used to perpetrate fraud. Respondents agreed that the ban would raise the barrier to entry for those engaging in illegal activities, making it more difficult for them to obtain and exploit SIM farms for fraud. However, they raised concerns that there were some potential legitimate uses for SIM farms captured by the Government’s definition of a SIM farm. The majority of respondents noted they did not object to the Secretary of State extending the ban to further articles in the future, subject to very clear parameters for the exercise of the Secretary of State’s powers such as consultation with relevant stakeholders.

[1] Fraud Strategy: stopping scams and protecting the public - GOV.UK (www.gov.uk)

[2] Ofcom, November 2022, Scams Survey

Methodology

The Government consultation included 30 questions organised under four themes:

A. Questions testing the proposed definition of SIM farms, their criminal use and possible legitimate uses [Q 1-7].

B. Questions exploring whether other technologies are used for fraud in the UK and should be brought under the proposed ban [Q8-13]

C. Questions assessing the conditions that might be put in place for a criminal offence to be committed in the supply, possession and/or use of SIM farms. [Q14 -22]

D. Questions assessing the conditions that might be put in place for a criminal offence to be committed in the supply, possession and/or use of other technologies [Q2326]

E. Questions seeking views on whether the Secretary of State ought to be able to extend the offence to other articles in the future [Q27-30]

The consultation included a further four questions under a Call for Evidence seeking information and data to allow more accurate estimates of the impacts on businesses [Q.31-34]. A final question [Q. 35] sought views in relation to impacts on people on the basis of protected characteristics under the Equality Act 2010.

We received a total of **50** responses to the consultation: 13 responses were submitted online and a further 37 were sent via email.

Table 1 below sets out a breakdown of responses by channel.

Response Channel	Number of Responses
Online	13
Word/PDF (received via email)	37
TOTAL	50

For the purpose of this response, we have grouped the respondents into eight categories, as shown in **table 2**.

Category	Number of Responses
Broadcast sector (inc. trade bodies)	15
Manufacturer/ Supplier	11
Member of the public	7
Telecoms sector (inc. operators, aggregators, trade bodies)	7

Law enforcement	4
Public sector (e.g. NHS)	2
NGOs	2
Other	2
TOTAL	50

Some respondents did not answer every question. As such, the number (and percentage) of answers to the questions often differ from the total number of responses received. Figures may also include some double counting where multiple views were expressed.

We are grateful to everyone who took the time to respond.

Summary of responses and Government response

Definition and uses of SIM farms and other technologies used for fraud in the UK (Q1-Q13)

Consultation responses

The first seven consultation questions sought views on the definition and uses of SIM farms. Q8-13 sought views on other technologies used for fraud in the UK. Responses to the consultation support the Government's aim to protect individuals and businesses from scams. However, they questioned the number of SIM card slots set in the definition and raised concerns that the definition could encompass legitimate uses. Similarly, they identified a number of other technologies used by businesses for legitimate purposes that could be abused by criminals.

Definition of SIM farms

The majority of respondents (34) disagreed with the Government's proposed definition of SIM farms, seven fully agreed and three agreed in part. Respondents questioned the number of proposed SIM card slots as the premise of the definition and were concerned the definition risked criminalising consumer devices such as smart phones that can hold up to eight eSIMs. eSIMs are downloadable digital profiles that act like a traditional physical SIM card. One response sought a more "future-proof and holistic definition" of SIM farms as "any means of sending bulk SMS other than via a regulated operator of bulk SMS channels".

Legitimate uses of SIM farms

A recurring concern amongst respondents was that the proposed definition was very broad and could encompass legitimate uses. Of the 29 responses we received to question 7, 18 said their business involved SIM farms.

Responses to the consultation identified the following legitimate uses of SIM farms:

i. Some multi-SIM devices are used in broadcast and programme making to facilitate the production and delivery of live and pre-recorded broadcasts. These are frequently data-only devices incapable of making calls or sending texts and can sometimes be referred to as 'bonded cellular technology'.

ii. Public Electronic Communications Networks (PECNs), as defined in the Communications Act 2003, are services people can sign up to in order to send electronic messages and use SIM farms to assess and maintain network security and network resilience. Relevant PECNs providers identified during the consultation include fixed-line operators, mobile network operators and internet service providers.

iii. SIM farms are used by transport providers to offer WiFi on trains, trams, buses, coaches or ferries as the devices switch between Mobile Network Operators (MNOs) depending on which network has best reception where the device is located at that moment.

iv. Emergency services use SIM farms to enable critical communications or send emergency alerts and messages to the public.

Criminal uses of SIM farms

We received 15 responses to question 3 (criminal use of SIM farms), which identified many criminal or illegitimate activities facilitated by SIM farms. SIM farms can be used for *"anything that an individual phone or SIM may be used for, just on a wider scale"*, including spam communications, scam texts and calls, data theft and fraud against telecoms operators:

i. A majority of respondents pointed to the use of SIM farms to circumvent legitimate communication channels and send calls and texts at significantly lower rates than the proper routes. This practice abuses telecommunication operators' terms of service and results in significant revenue loss to both operators and legitimate SMS suppliers.

ii. The second most mentioned illegitimate activity was the use of SIM farms for fraud attempts via texts and messages. SIM farms are used to send scam texts at scale, robo-calling campaigns and live calls to harvest personal information to trick victims into transferring money out of their accounts. Respondents linked SIM farms to scam messages such as the 'Hi Mum', 'missed parcel delivery' and 'suspicious transaction' scam texts, all examples of 'smishing' (SMS phishing). SIM farms are also used to send unsolicited marketing texts and calls (spam) at low rates. As one MNO respondent noted, SIM farms 'generate very large quantities of outgoing messages, so that even if only a small proportion fall for the deception, the absolute number is still quite significant'.

It is worth noting that SIM farms can also cause harmful interference to the operation of mobile networks, causing congestion and a reduction in service quality.

iii. Where SIM farms are used for business communications by supposedly legitimate businesses, although doing this is in breach of the terms of service, they also contribute to privacy risks by collecting and storing sensitive data, with potential for unauthorised access and compliance breaches. Device operators can access the content of legitimate SMS going through the equipment, harvest the data it contains or manipulate its content to form phishing attacks.

iv. SIM farms also enable the creation of fake and/or automated accounts on online platforms which criminals use to spread misinformation and harmful messages.

More widely, respondents said SIM farms can be used to commission and co-ordinate any type of criminal activity.

Other technologies used for fraud

When asked what other technology could be brought under this ban, respondents pointed to the chaining of devices, ‘Cash for SMS’ apps and virtual SIM hosting. They suggested multiple devices such as other types of GSM modems, phones or 4-slot SIM farms could be wired together in series to create a multi-slot SIM farm.

Mobile apps that allow users to sell their unused free SMS messages - ‘Cash for SMS’ apps - were described as a key technology already in use. These apps can be used to automate and scale SMS scam and spam activities and their use is likely to grow as SIM farm use is reduced.

Respondents suggested that SIM servers should be covered in this ban as they are highly sophisticated and likely in wider use due to their functionality:

> “Virtual SIM hosting is a technique employed in SIM farms where International Subscriber Mobile Identity (IMSI) components are uploaded onto servers or hardware. This allows for simultaneous operation of multiple SIMs on a single server or cluster” [Telecoms Operator]

A few responses noted that banning physical SIM farms alone is likely to result in displacement to eSIM farms. However they acknowledged that if eSIMs were included to the proposed ban, the Government’s definition of SIM farms should be adapted to ensure it excludes smartphones that can hold more than four eSIMs.

Respondents suggested the proposed ban should consider all the channels that bad actors have access to such as chat apps and social media. They said the following technologies could be used for fraud:

i. forms of digital technology such as iSpoof and other websites that advertise spoofed SMS or voice calls – these do not rely on SIM cards or other physical equipment.

ii. Application-to-person (A2P) services, which are online bulk SMS messaging services, that offer free trials and/or do not conduct sufficient customer checks can be abused by fraudsters to send fraudulent SMS messages.

iii. combining burner phones with SMS casting software (software used by businesses to send texts to multiple customers at once), such as connecting handsets to a computer and using SMS casting software to send out scam texts.

iv. Cyber-attacks against the global signalling network between mobile operators, often referred-to as Signalling System Seven or SS7. SS7 attacks allow criminals to compromise and intercept voice and SMS communications, such as banking SMS messages.

v. Abuse of Voice over Internet Provider (VoIP) apps such as Skype and Hashed, for example by compromising and using VoIP credentials of legitimate businesses.

While not proposing an outright ban, respondents also noted that the

> “Use of [Over-The-Top or messaging over data] Apps like WhatsApp, Viper, WeChat. Facebook Messenger, iMessage to send phishing traffic could grow unchecked if the Government are not applying appropriate measures to ensure the vendors have control over their services” [Communications Provider]

Respondents noted that while most of these technologies could be abused by criminals, they are also used by businesses for legitimate purposes. For example, they noted that platforms like Skype (which offers to send volume texts) are legal, and A2P SMS plays a vital role in facilitating effective communication between business and the general population.

Government response:

We welcome the confirmation that SIM farms are frequently used to perpetrate fraud at a vast scale. However, we also recognise that the proposed definition could capture a number of legitimate businesses.

Our primary objective is to stop criminals accessing SIM farms – it is not our intention to disrupt legitimate business or hinder technological development in the UK. For that reason, we will ensure that the definition of SIM farms takes into account the concerns raised.

In particular, our definition will capture devices that contain or incorporate five or more physical SIM cards for the purpose of making calls and/or sending SMS texts. However, we will exempt any data-only devices that are not capable of making calls or sending texts. We will ensure that a ban includes a defence for legitimate uses that will mean that legitimate businesses possessing or supplying SIM farms are not adversely affected, such as the broadcast and transport industries. It will also not apply to the Crown.

Responses noted that the definition could also include eSIMs and mobile apps. However, we did not receive sufficient evidence at consultation to include them in a proposed ban, due to their complexity and ongoing pace of development. This could be further addressed by the proposed powers to extend the ban to other forms of telecommunications equipment and articles used to perpetrate fraud (below).

Proposal to ban the manufacture, import, sale, hire, possession and/or use of SIM farms and other technologies in the UK (Q14-Q26)

Consultation responses

Of 45 responses, 24.4% fully agreed with the ban, 24.4% agreed in part with the ban, 48.8% disagreed with all elements of the ban and 2.2% remained neutral. Whilst supportive of the Government’s aim to reduce fraud, those who disagreed either felt that the ban was not the best solution and suggested alternatives or felt that it would disproportionately impact UK businesses.

The majority of consultees did not comment on the strict liability aspect of the offence. Of those who did, the majority (7 responses) were in favour while 5 noted it was not proportionate to the offence. Nine participants commented on the proposed penalty of an unlimited fine, with four suggesting a custodial sentence would be more appropriate and one proposing confiscation of assets in addition to a prison sentence. One respondent noted the need for exemptions to any proposed sentence, to protect those using the devices for legitimate reasons.

Responses to Q23-Q26 of the consultation did not comment on the possible impact of a ban of other technologies used for fraud in the UK, beyond where this would impact on the broadcast and other industries. Information and data provided in this section has been incorporated into the call for evidence and the impact assessment.

Impact on businesses

27 responses to the consultation raised concerns about the impact of the proposals on broadcast and other sectors that use SIM farms and other multi-SIM devices for their operations, as set out earlier.

In particular, there were extensive concerns the ban would negatively affect the ability of broadcasters, programme makers and live content producers to cover news programming and provide live feeds from various events to wide audiences (19 responses). Two respondents also noted the ban would restrict the ability of telecoms operators and thirdparty service providers to support service testing on UK telecommunications networks.

Respondents acknowledged the proposals would impact uses that already violate mobile network terms and conditions, such as the use of SIM farms for Business-to-Customer communications (4 responses). However, others were confident that the legitimate use of devices that house multiple SIMs, such as ensuring continuity of connection in areas of insufficient signal coverage, would not be affected and that suitable alternatives were available. Where no direct alternative is available, respondents felt that the positive impact of the ban should outweigh the negative impact (5 responses).

Impact on fraud

Responses regarding the impact of the ban on criminal uses were split equally between those who expected a positive impact (8 responses) and those who questioned its efficiency (8 responses). Respondents said the ban would contribute to a more secure and trustworthy digital ecosystem and help mitigate fraud. It would raise the barrier of entry for criminals, which in turn should result in fewer scam texts even if it did not completely stop them. They also felt enforcement of the ban would work as a deterrent to criminals considering SIM farms as a means for fraud. However, others felt the ban did not go far enough and would not completely stop fraudsters from abusing telecommunications networks to commit fraud.

The consultation asked for views on other ways to prevent the criminal use of SIM farms and protect the public from mass text scams. Six responses asked for greater responsibility on MNOs to monitor their networks for signs of fraudulent activity. For example, they should screen and block messages containing spam or suspicious URLs; and use modern technology, including AI, to detect and prevent such activity, ensuring the integrity of network services without impacting legitimate users. Enhanced security measures, improved network control, and reduced anonymity could make fraudulent operations more challenging to conduct. Six responses suggested a licensing regime for legitimate use cases.

Four responses also called for a change in SIM card policy, with some form of proportionate registration or verification measures to be considered to allow a degree of flexibility for genuine consumers, while making it difficult for criminals to purchase large numbers of SIM cards. Pre-registration of SIM cards at the point of purchase, due diligence checks by UK operators on the supply chain of their SIM cards and the removal of 'unlimited SMS' packages were also recommended to make bulk sales safer and the abuse of SIM cards harder. One response called for official registration of business phone numbers to specified users and physical locations to address spoofing. A common thread in responses was the need to focus on prevention, such as information sharing to identify bad actors, and co-ordinated efforts to raise public awareness about telecommunications and telecommunications-related fraud.

Finally, respondents proposed classing SIM farms as articles for use in fraud under sections 6 and 7 of the Fraud Act and requiring online platforms to remove adverts that promote the supply of technology such as SIM farms.

Government response

We welcome the broad support in favour of restricting access to SIM farms. Some respondents noted that there are alternatives to a ban, such as licensing. However, our view is that a criminal offence would be more proportionate in line with the criminal nature of the activity that SIM farms can facilitate, and that licensing would actually be more burdensome for businesses than an exemption for legitimate uses.

We note views that the ban may not be fully effective in preventing criminals from accessing and deploying SIM farms. A ban on sale and possession will mean that these Similarly, a ban would give law enforcement greater ability to detect and disrupt use of SIM farms and give further investigatory opportunities which may lead to prosecution for other crimes that were enabled by the use of SIM farms, for instance fraud or money laundering.

We are very grateful for further suggestions to tackle telecommunications-enabled fraud, which we will continue reviewing. The Government continues to work closely with the telecommunications industry to reduce fraud. Fraudulent messaging through apps is addressed through the Online Safety Bill as well as the Government’s ongoing work with the tech industry. Finally, the Government is separately reviewing the operation of the bulk messaging sector with a view to disrupting fraudsters using bulk messaging to send large volumes of scam texts.

Ability to add further items to the list of banned technologies (Q27-Q30)

Consultation responses

We received 22 responses regarding the exercise of the Secretary of State’s powers to be able to extend the proposed ban to other technologies in the future. 27% of those who responded did not agree with the proposals while 73% agreed with the proposed powers, subject to clear parameters for the exercise of the Secretary of State’s powers.

Those who disagreed were concerned that simply adding to the list of banned articles would negatively impact the UK economy while others raised concerns about the concentration of power to the Government, rather than Parliament, and an open-ended power to define other technologies that may be brought under the ban.

The majority of respondents emphasised the need for a wide and full consultation with stakeholders prior to making any changes to the list of banned items.

Government response

The Government considers it important to ensure that the ban is flexible and can be used to rapidly prohibit other types of technology where these are identified in the future. Some such technologies are mentioned above, whilst others may emerge in future and the Government will continue to review fraud methodologies closely for changing patterns and new technologies being used, such as eSIM farms and others. However, the Government agrees with respondents that any powers to ban through secondary legislation ought to have clear parameters for their use.

We will ensure that any powers in this area will be carefully drafted and will be limited to cases where there is significant evidence of the use of particular technologies for fraud, and also include a requirement for a public consultation.

Call for Evidence

A call for evidence (Questions 31-34) was included in the consultation to collect information and data that would have allowed more accurate estimates of potential impacts of a ban. The consultation responses included some information and evidence but not enough to provide a comprehensive assessment of the impact of a potential ban.

Limited information and data on the potential legitimate use cases of SIM farms was provided. The information that was provided has been taken into account as part of the policy design to ensure that impacts on legitimate businesses are minimised.

Mobile network operators (MNOs) provided evidence on the volumes of suspected scam texts sent on their networks and said that they believe criminals use SIM farms to facilitate this activity. SIM farms lead to a negative consumer experience due to network congestion.

A ban would be expected to reduce the level of fraud, and the corresponding socioeconomic harms. However, due to the limited amount of evidence received, there remain uncertainties in relation to the impact of the proposals to businesses and the costs associated with introducing and implementing the ban. Therefore, the cost and benefit estimates of the policy impact, are largely qualitatively assessed in the Impact Assessment which will be published alongside any proposed legislation.

Annex A: Questionnaire

A. Definition and uses of SIM farms

Q1. Do you agree with the government definition of a SIM farm, as a device that contains more than four SIM cards?

Please explain your answer and give evidence where possible (Max. 250 words)

Q2. What other technology could be brought under this ban and how should this be described?

Please explain your answer and give evidence where possible (Max. 250 words) Q3.

What crimes are SIM farms used to facilitate?

Please explain your answer and give evidence where possible (Max. 250 words)

Q4. Do you have any data or examples to demonstrate the scale of their illegitimate uses?

Please explain your answer and give evidence where possible (Max. 250 words)

Q5. Are you aware of legitimate uses of SIM farms that are not mentioned in this document?

Please explain your answer and give evidence where possible (Max. 250 words)

Q6. Do you have any data or examples to demonstrate the scale of their legitimate use?

B. Other technologies used for fraud in the UK.

Q8. Do you know of any other technologies, services or devices, online or offline, that can be used to do similar things as SIM farms? How easy would it be to switch to these?

Please explain your answer and give evidence where possible (Max. 250

words) Q9. Are you aware of any legitimate uses of the items specified in Q8?

a) Yes

b) No

Please explain your answer and give evidence where possible (Max. 250 words) Q10. [For businesses] Does your business involve any of the items specified in Q8?

a) Yes
b) No

Please explain your answer and give evidence where possible (Max. 250 words)

Q11. Do you know any other technologies, services or devices, online and/or offline, that can be used to send scam texts and/or make scam calls? a) Yes

b) No

Please explain your answer and give evidence where possible (Max. 250 words)

Q12. Are you aware of any legitimate uses of the items specified in Q11? a) Yes

b) No

Please explain your answer and give evidence where possible (Max. 250 words) Q13.

[For businesses] Does your business involve any of the items specified in Q11? a)

Yes

b) No

Please explain your answer and give evidence where possible (Max. 250 words)

C. Proposal to ban the manufacture, import, sale, hire, possession and/or use of SIM farms in the UK:

Q14. To what extent do you agree with the proposal to ban the manufacture, import, sale, hire, possession and/or use of SIM farms in the UK?

a) Yes – fully agree
b) Yes – agree in part/ not all aspects of ban
c) No – disagree
d) Don't know

Please explain your answer and give evidence where possible (Max. 250 words)

Q15. Should this be a strict liability offence (i.e. the offender is held accountable for the manufacture, import, sale, hire, possession and/or use of SIM farms regardless of whether they behaved with the intention to commit a crime or with negligence)?

Please explain your answer and give evidence where possible (Max. 250 words)

Q16. Should the punishment for this offence be an unlimited fine or what other punishment would be proportionate?

Q17. How would banning SIM farms impact their legitimate uses (if any)? Please

explain your answer and give evidence where possible (Max. 250 words) Q18.

How would banning SIM farms impact their illegitimate or criminal uses?

Please explain your answer and give evidence where possible (Max. 250 words)

Q19. Are you aware of any groups of businesses, organisations and/ or individuals that will be particularly affected by these proposals?

a) Yes
b) No
c) Don't know

Please explain your answer and give evidence where possible (Max. 250 words)

Q20. Are there any other means to prevent criminals abusing SIM farms that could

also achieve the goal of protecting the public from mass text scams? a) Yes

b) No

Please explain your answer and give evidence where possible (Max. 250 words)

Q21. What would be the impact of this proposal to ban the manufacture, import, sale, hire, possession and/or use of SIM farms in the UK on your business or organisation if it came into force?

Please explain your answer and give evidence where possible (Max. 250 words)

Q22. Should a short, and strictly limited period of time, transition period be set to

allow businesses, organisations and individuals to remove SIM farms? a) Yes

b) No

Please explain your answer and give evidence where possible (Max. 250 words)

D. Proposals to ban the manufacture, import, sale, hire, possession and/or use of (other) technologies used for fraud in the UK.

Q23. Are you aware of any impact our proposals to ban the manufacture, import, sale, hire, possession and/or use of (other) technologies used for fraud in the UK may have, that we have not captured in this document?

a) Yes

b) No

Please explain your answer and give evidence where possible (Max. 250 words)

Q24. Are you aware of any groups of businesses, organisations and/ or individuals that will be particularly affected by the proposal to ban other technologies? a) Yes

b) No

Please explain your answer and give evidence where possible (Max. 250 words)

Q25. What would be the impact of the proposal to ban other technologies used for fraud in the UK on your business or organisation if it came into force?

Please explain your answer and give evidence where possible (Max. 250 words)

Q26. Do you have any comments or further information to add to the published economic note to further inform our proposals?

a) Yes
b) No

Please explain your answer and give evidence where possible (Max. 250 words)

E. Ability to add further items to the list of banned technologies.

Q27. Should the Secretary of State be able to add items to the list of banned technologies in the future?

a) Yes
b) No

Please explain your answer and give evidence where possible (Max. 250 words)

Q28. Are conditions of evidence of use, stakeholder consultation and affirmative procedure the appropriate for adding items to the list of banned technologies? (More information about the affirmative procedure is available at https://guidetoprocedure.parliament.uk/articles/ovuiEncc/what-happens-tostatutoryinstruments-under-the-affirmative-procedure)

Please explain your answer and give evidence where possible (Max. 250 words)

Q29. We propose that the Secretary of State be able to add items to the list of banned technologies in the future. Are you aware of any impact this proposal may have, that we have not captured in this document?

a) Yes
b) No

Please explain your answer and give evidence where possible (Max. 250 words)

Q30. Are you aware of any groups any groups of businesses, organisations and/

or individuals that will be particularly affected by this proposal? a) Yes

b) No

Please explain your answer and give evidence where possible (Max. 250 words)

F. Call for Evidence

Q31. Do you have any data or evidence to demonstrate the scale of legitimate use of SIM farms and other technologies used to communicate at scale?

Q32. Do you have any data or evidence to demonstrate the scale of the illegitimate use of SIM farms and similar technologies?

Q33. How would banning SIM farms impact their legitimate and illegitimate use?

Q34. Are you aware of any impact the proposals may have that we have not captured in the economic impact note, published alongside this document?

Equality Impacts

Q33. Do you have any comments about the proposals in this consultation document in relation to impacts on people on the basis of any of the following protected characteristics under the Equality Act 2010: age; disability; pregnancy and maternity; race; religion or belief; sex; sexual orientation and gender reassignment; marriage or civil partnership? How might such impacts be mitigated? (Max. 500 words)

E03015619

978-1-5286-4563-8