Home Office

Preventing the use of SIM farms for fraud

Government consultation

This consultation and call for evidence begins on 03 May 2023

This consultation and call for evidence ends on 14 June 2023

CP 843

Preventing the use of SIM farms for fraud

Government Consultation

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

May 2023

CP 843

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

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

ISBN 978-1-5286-4099-2

E02907078 05/23

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.

About this consultation

To:	This consultation is open to the public and is targeted at victims and businesses who are victims of fraud, including from scam texts and scam calls. We are particularly interested to hear from those who may be affected by the proposals, should they become legislation, including telecommunications operators, businesses, law enforcement, consumer groups, as well as non-governmental organisations with a focus on fraud victim, civil liberties and human rights groups.
Duration:	6 weeks from 3 May 2023 to 14 June 2023
Enquiries to:	SIM farm Consultation Economic Crime Directorate Homeland Security Group Home Office 6th Floor, Peel Building 2 Marsham Street London SW1P 4DF Email: SIMfarmConsultation@homeoffice.gov.uk
How to respond:	Please send your response by 17:00 on 14 June 2023 via email at SIMfarmConsultation@homeoffice.gov.uk
Additional ways to respond:	If you are unable to respond by email, you can download a PDF version of the online form and submit it by email or post. If you require information in another format, please email: SIMfarmConsultation@homeoffice.gov.uk. Please tell us what format you need. It will help us if you say what assistive technology you use. We may not be able to analyse responses not submitted in these provided formats.
Response paper:	A response to this consultation and call for evidence will be published on gov.uk after the consultation is complete.

Contents

Ministerial Foreword

As Home Secretary, protecting the public is my highest priority and fraud is the biggest crime in the UK. Today, I have published a Fraud Strategy setting out the government's ambition to cut fraud by 10% from 2019 levels, down to 3.33 million frauds by the end of 2024. To do this, it is crucial we stop scams from reaching people in the first place.

Fraudsters use technology and communications that are ubiquitous in everyday life, such as texts and phone calls, to contact people so they can trick them into handing over their money. To prevent the devastating financial and emotional harm this causes, we must deny criminals access to any tool that allows them to send bulk messages or make scam calls.

This is why I am launching this consultation on banning the supply and use of SIM farms in the UK. To make the proposals future proof, we are also asking what other technologies should be banned to prevent criminals being able to use them for fraud.

These proposals pave the way for future legislation to improve the response to telecommunications-enabled fraud, to ensure that our law enforcement agencies remain ahead of the curve and to leave criminals with no place to hide.

Rt Hon Suella Braverman KC MP

Home Secretary

Executive Summary

SIM farms are devices that can house hundreds of SIM cards, which can send out thousands of scam texts to defraud the UK public of millions of pounds. In addition to sending scam texts, these devices are used by criminals to run scam call campaigns and to post misleading, false or phishing messages on social media in bulk. Criminals use them to mask communications data when making calls or texts, making investigations significantly more difficult. SIM farms are frequently used in abuse of telecommunications operators' terms of service to send legitimate traffic at significantly cheaper rates than if this was done through the proper routes.

Whilst there are some potentially legitimate uses of the technology, these are limited and should not require using more than four SIM cards, based on the number of mobile operators in the UK. We have very limited evidence that there are any legitimate use cases for devices that allow the use of more than four SIM cards, and for all such cases alternative options exist.

This consultation sets out proposals to ban the manufacture, import, sale, hire and possession of SIM farms (devices for more than four SIM cards) in the UK. In addition, we are asking whether other technologies used almost exclusively to commit fraud should be included. We are also seeking input on our definition of SIM farms to ensure it accurately captures the devices currently in use, and views on our option to apply the measure only to devices with more than four slots.

To ensure we can respond to new threats we identify in the future, the consultation is also seeking views on whether the Government should be able to update the list of banned technologies and articles through secondary legislation.

To mitigate any costs arising from the proposals, we are asking whether we should set a period of time to allow organisations to evaluate the processes and technology they use and transition to alternative methods.

Alongside this, we are launching a call for evidence to collect information and data that will allow more accurate estimates of the impacts on businesses to be made. A detailed appraisal will be completed, and a full Impact Assessment provided following the consultation.

Background

The threat to the UK public from fraud

As set out in the recent Fraud Strategy, fraud is increasing as a proportion of crime and now accounts for over 40% of all estimated crime in England and Wales.[1] In the year ending December 2022 there were 3.7 million estimated fraud offences, and 1 in 15 adults were a victim of fraud. In the year ending March 2022 18% were victims of fraud on more than one occasion.[2] The cost of fraud is staggering. The total cost to society of fraud against individuals in England and Wales was estimated to be at least £6.8 billion in 2019-20.[3] This includes the money lost by victims, the cost of supporting victims, and the costs of recovery, investigation and prosecution of fraudsters.

One reason for this rapid increase in the scale and harm from fraud is increasing complexity and technological sophistication of the tools available to fraudsters both in the UK and overseas. Criminals often abuse telecommunication networks to target people and defraud victims at significant scale. In the period June-August 2022, three quarters of people in the UK said they had received a suspicious message, in the form of either a text, a recorded message or a live voice call to a mobile. This represents over an estimated 40.8 million adults in the UK.[4] An estimated 700,000 then followed the scammer's instructions, risking financial loss and significant emotional distress.

Case study: Missed Delivery Text Scam
A 20-year-old female, Gemma*, who had recently lost her mother, received a scam text purporting to be from Royal Mail. She clicked on the link, gave her details, and paid a fee for redelivery. The next day she received a call claiming to be from the FCA and was told her passwords had been stolen and someone was trying to transfer money from her bank, so she should transfer all her money to a 'safe' account. She was panicked into transferring £9,200 she had inherited from her mum, suffering anxiety and panic attacks after realising she was a victim of fraud.

What could banning SIM farms do here? Banning SIM farms would help stop criminals being able to instantly send thousands of spam messages by these means. Measures have been set out in the Fraud Strategy to give the regulators powers to make banks and financial firms reimburse victims like Gemma, reducing the emotional and financial harm.

*name has been changed

[1] TCSEW year ending December 2022

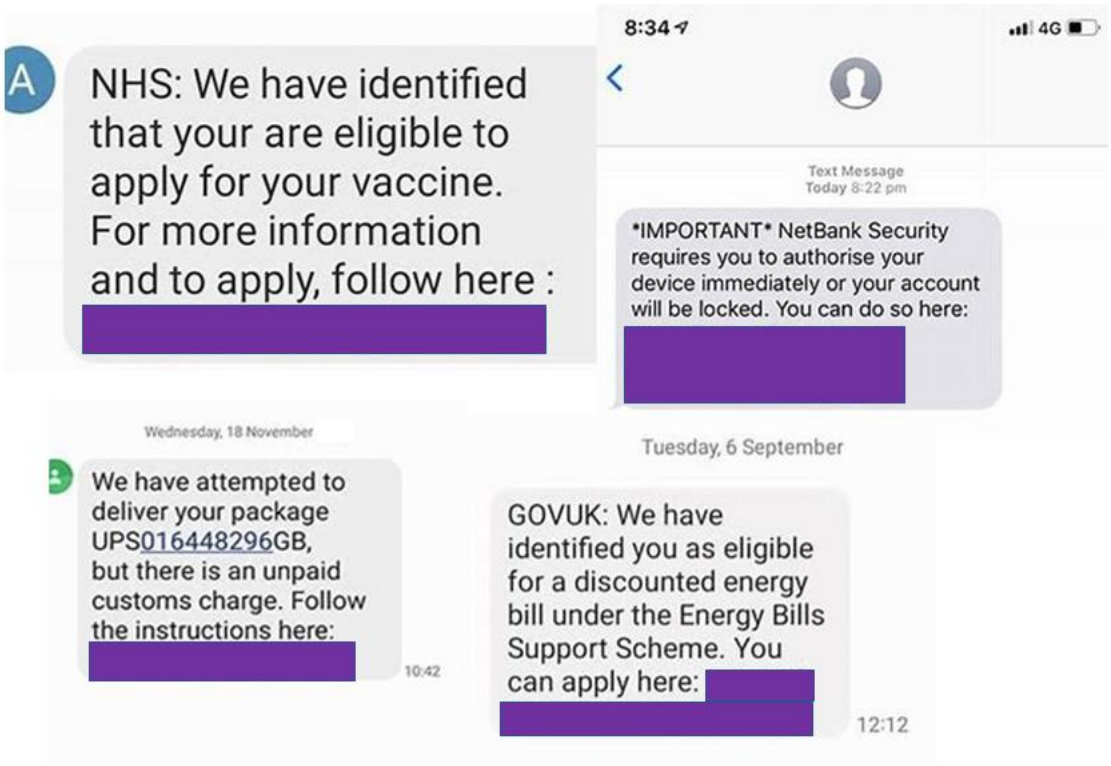
[2] TCSEW year ending March 2022 Crime in England and Wales: Appendix tables - Office for National Statistics (ons.gov.uk): Table A3

[3] The Economic and Social Costs of Crime 2022. This figure estimates wider costs to society including preventative spending, emotional harms and the law enforcement response to fraud committed against individuals.

[4] Ofcom, November 2022, Scams Survey

Scam texts

Texts are the most common form of suspicious message with more than 6 in 10 people reporting that they had received suspicious texts. Reports of suspicious calls are lower but still significant: 21% of respondents reported suspicious live calls to their mobiles and 19% to their landlines[5]. Scam texts are frequently traced back to SIM farms and other technologies that allow criminals to send out scam messages in bulk. The Government is committed to stopping criminals from exploiting technologies and equipment, such as SIM farms, and to secure our telecommunications networks from those seeking to defraud the UK public.



Current legal position

Existing legislation does not prevent criminals from obtaining and using SIM farms, and other similar technologies. The Fraud Act makes it illegal to supply or possess articles, including SIM farms, if they are intended to be used for fraud. However, it is extremely difficult to establish that a person who possesses, makes or supplies SIM farms is intending to use them for fraud. Likewise, the Act does not require importers, manufacturers or sellers to undertake checks on the intended use of the device.

Under the Wireless Telegraphy Act 2006 (WTA), Ofcom and the Secretary of State have powers to impose restrictions if an article interferes with wireless telegraphy. These powers do not apply to crime or national security (only wireless interference), meaning that is not possible to use them to prevent abuse of wireless telegraphy to commit fraud, such as to tackle SIM farms.

[5] Ofcom, November 2022, Scams Survey

This means that criminals, already intent on breaking the law, do not face any barriers in terms of procuring SIM farms to conduct their criminal activities. This is why we are introducing new measures to make it as difficult as possible for criminals to obtain and use SIM farms in the UK.

SIM farms can also present in the form of a mobile app which either offers to pay users for their unused free SMS messages or installs malware that steals their SMS allocation every month. In December 2022 the Government published a voluntary Code of Practice[6] which set out minimum security and privacy requirements for app store operators and app developers. The Code of Practice for App Store Operators and App Developers aims to protect users from malicious and poorly developed apps and will address the risks from app versions of SIM farms. We are monitoring the implementation of this and will consider what more needs to be done to disrupt the app version of SIM farms, including through the use of the relevant measures outlined in this consultation document.

[6] https://www.gov.uk/government/publications/code-of-practice-for-app-store-operators-and-app-developers

Consultation: The threat to the UK public from SIM farms and similar technologies

Definition of SIM farms

There are many different names for SIM farms, including SIM boxes, SIM gateways, Global System for Mobile communication (GSM) gateways, Voice over Internet Protocol (VoIP) gateways, and SMS gateways.

These are devices that convert fixed-line (internet or public switched telephone network) communications into mobile communications. Their primary use is receiving calls or SMS messages sent over the internet and re-transmitting them over mobile networks to be able to reach mobile phones.[7] Businesses can use them to ensure continuity of connection when moving through areas of insufficient signal coverage; or meet short-term communication needs without the need to install a permanent fixed line to temporary sites. A call or text sent from these devices appears to the mobile network to have originated from a mobile phone registered to that network.[8]

There are substantively only four mobile operators in the UK, with all other providers piggybacking off their services. This means that devices with five or more SIM slots are not required to ensure continuity of connectivity. They can be used differently, such as to repeatedly access the network to send mass texts, to make many calls, or to access the internet through many connections. In this consultation, we therefore define SIM farms as devices with more than four slots.

We recognise the above definition refers mainly to physical devices and may be missing other iterations of the technology, including possible combinations of physical hardware and virtual software. Therefore, to ensure we have accurately captured all iterations of a SIM farms, we invite views on this definition.

Questions to consultees:

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

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

[7] Future regulation of GSM gateways under the Wireless Telegraphy Act (ofcom.org.uk); See also: "http://www.bailii.org/ew/cases/EWCA/Civ/2009/47.html"Office of Communications T-Mobile (UK) Ltd v Floe Telecom Ltd [2009] EWCA Civ 47 (10 February 2009) (bailii.org) - para 27.

[8] Future regulation of GSM gateways under the Wireless Telegraphy Act (ofcom.org.uk)

The threat

Scam texts are frequently traced back to SIM farms, which can sometimes house hundreds or thousands of SIM cards. 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 attractive, easy to access, low-cost option to criminals who send out large volumes of texts to phish[9] for sensitive data, like bank details.

SIM farms allow criminals to use all capabilities of SIM cards in bulk and at low cost. In addition to sending huge numbers of scam texts, this includes running scam call campaigns and posting misleading, false or phishing messages on social media in bulk. The technology can also allow criminals to conceal communications by showing inaccurate Caller Line Identification (CLI) data and incorrect caller location.

SIM farms are openly advertised on popular online marketplaces for purchase and shipping to the UK. The majority of marketplaces have very limited to non-existent checks to verify the identity of their customers. This means that it is extremely easy for criminals to obtain SIM farms, at a low-cost, and use them to target the UK public.

It is not possible to establish the exact number of SIM farms being used, but fraud statistics indicate that the use of SIM farms was amongst the top five types of telecommunications fraud in 2021.[10] For example, one police investigation discovered that five SIMs had sent over 900,000 messages in one SIM farm between April and October in one year.

Scam messages continue to get past the mobile network's filters. This is because, in response to detection efforts, SIM farm techniques are evolving rapidly. Some SIM farm providers explicitly offer methods to counteract detection strategies, such as specialist software that imitates the way humans use SIM cards in their mobile phones (Human Behaviour Simulation software). For example, SIM cards in the SIM farm may call or text other SIM cards in the box, rendering the SIM card's behaviour appear as more 'normal'. Such methods aim to bypass the controls in place by mobile operators and make SIM farms much harder to detect.

Application-to-person (A2P) messaging, such as automated appointment reminders, two-factor authentication prompts or sending bulk SMS as part of marketing campaigns, are an increasingly important part of the overall SMS market. Whilst usually against the telecommunications provider's terms of service, some unscrupulous actors also funnel A2P messaging through SIM farms in order to reduce their costs, causing losses to the legitimate operation of the provider.

To inform our proposals, we are seeking views and evidence on these and other threats posed by SIM farms.

---

[9] text messages that deceive victims into giving sensitive information to a disguised attacker

[10] C. F. C. Association, "Fraud Loss Survey Report 2021," Communications Fraud Control Association, 2021 - CFCA 2021 Fraud Loss Survey – CFCA

Questions to consultees

Q3. What crimes are SIM farms used to facilitate?

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

Legitimate uses

We have identified a limited set of legitimate use cases for devices that house four or fewer SIM cards, such as to ensure continuity of connection when moving through areas of insufficient signal coverage or to meet short-term communication needs without the need to install a permanent fixed line to temporary sites.

However, we have engaged extensively across industry and law enforcement and have not identified any legitimate use case for SIM farms (defined as devices with more than four slots). Any of the above legitimate use cases do not require such a configuration and in all cases alternative options likely exist.

It is currently legal in the UK for businesses or consumers to buy, install and use SIM farms for personal use, in a set-up known as Single-Use GSM Gateways. However, as upheld by the Supreme Court on 8 March 2023, their set-up in a commercial multi-user format (known as COMUGs) requires an Ofcom licence. Ofcom have never issued a licence, meaning that it is not legal to operate a COMUG. However, the sale of SIM farms, which can easily be set up as COMUGs, remains unrestricted and they are sold openly on online marketplaces, meaning criminals can continue to easily obtain and operate them. The way COMUGs are used allows their operators to conceal communications data should they choose to. This makes it more difficult for law enforcement to investigate criminals and identify and locate people at risk of harm.

We invite views for information on any legitimate uses for SIM farms that are not listed above.

Questions to consultees:

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

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

Q7. [**For businesses**] Does your business involve SIM farms?
a) Yes
b) No

Criminals also use other technologies to target their victims

iSpoof

iSpoof is a website that offered services that enabled those who signed up to and paid a fee to make spoofed calls, send recorded messages and intercept one-time passwords. This enabled criminals to impersonate trusted, legitimate businesses and carry out social engineering attacks.

iSpoof had around 59,000 users, which caused £48 million of losses to 200,000 identified victims in the UK. One victim was scammed out of £3 million, while the average amount stolen was £10,000.

In the 12 months before August 2022, about 10 million fraudulent calls were made globally using the service.

Fraudsters paid between £150 and £5,000 a month to use the iSpoof service, contacting, at times, 20 people a minute, mainly in the United States, UK, Netherlands, Australia, France and Ireland.

The investigation was led by the Metropolitan Police in collaboration with the City of London Police, the National Crime Agency and law enforcement agencies in Australia, Canada, France, Germany, Ireland, Lithuania, Netherlands, Ukraine and the USA.

We are conscious that there are other methods available to criminals to contact their victims - and as technology continues to develop more will emerge in the future. The recent iSpoof case shows these can take many forms and are not restricted to physical devices. It also shows that technologies available to fraudsters go beyond SMS, extending to making spoofed voice calls, sending recorded messages and intercepting one-time passwords.

While iSpoof has now been shut down, it shows the adaptability, and the pace of innovation criminals are capable of. This is why we are seeking views on other technologies used by fraudsters.

Questions to consultees

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?

Q9. Are you aware of any legitimate uses of the items specified in Q8?
a) Yes
b) No

Q10. [**For businesses**] Does your business involve any of the items specified in Q8?
a) Yes
b) No

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

Q12. Are you aware of any legitimate uses of the items specified in Q11?
a) Yes
b) No

Q13. [**For businesses**] Does your business involve any of the items specified in Q11?
a) Yes
b) No

Proposed new offence

We intend to create a criminal offence to ban the manufacture, import, sale, let or hire, possession and/or use of technologies used for fraud in the UK. The legislation will list the technologies identified by this consultation, including SIM farms.

We propose that this would be a strict liability offence, meaning it would not be necessary to show that the accused knew, or had reasonable grounds to suspect, that the SIM farm would be used in crime, including fraud. We propose that this offence would carry the penalty of an unlimited fine but that it would not carry the risk of custodial punishment. We invite views on whether this is proportionate.

The intention is that the offence applies to the whole of the UK. Whilst, the detection, investigation and prosecution of fraud are devolved, telecommunications policy and what communications devices and services are lawful are a reserved matter for the UK Parliament. However, regulation of wider technologies is devolved in some parts of the UK and we continue to engage with devolved authorities on this.

We are keen to hear views on the proposed offence and whether there are alternative means to prevent criminals abusing SIM farms that could better protect the public from mass scam texts.

Questions to consultees

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

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)?

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)?

Q18. How would banning SIM farms impact their illegitimate or criminal uses?

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

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

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?

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

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

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

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?

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

Ability to add further articles to the list

While we are consulting with a wide range of stakeholders, we do not believe it is possible to compile an exhaustive list of items, beyond SIM farms, to list at introduction of the proposed ban.

Fraudsters can be quick to adapt and we want to ensure that these provisions can be adjusted accordingly. We therefore propose the Secretary of State would be able to amend the list to add a new item in future, if there is evidence that the technology is used in fraud.

We propose that the Secretary of State can add an item to the list if it is involved in fraud and the following conditions are met:

- There is evidence of criminal use including the carrying out of fraud
- Stakeholders and parties affected by the change have been consulted, and
- Parliament approves the amendment via affirmative procedure[11].

We invite views on these provisions and whether they ensure proportionality.

Questions to consultees

Q27. Should the Secretary of State be able to add items to the list of banned technologies in the future?
a) Yes
b) No

Q28. Are conditions of evidence of use, stakeholder consultation and affirmative procedure appropriate for adding items to the list of banned technologies?

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

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

[11] More information about the affirmative procedure is available at https://guidetoprocedure.parliament.uk/articles/ovuiEncc/what-happens-to-statutory-instruments-under-the-affirmative-procedure

Call for evidence for additional information

We do not have a full picture of the impact of the proposals on businesses and the costs associated with introducing and implementing the ban due to lack of sufficient evidence. Therefore, alongside the consultation, we are issuing a call for evidence to collect information and data that will allow more accurate estimates of the impacts on businesses.

We invite all interested parties to provide feedback and empirical evidence on the benefits, unintended effects, consistency and coherence of the framework under which SIM farms are made available and operated in the UK.

We will produce a full Impact Assessment using the information returned to this 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?

Questionnaire

About you

Please use this section to tell us about yourself:

Full name	
Job title or capacity in which you are responding to this consultation exercise (for example, member of the public, law enforcement agency, legal professional, industry professional etc.)	
Date	
Company name/organisation (if applicable)	
Email address	
Address Postcode	
If you would like us to acknowledge receipt of your response, please tick this box	
Address to which the acknowledgement should be sent, if different from above	

If you are a representative of a group, please tell us the name of the group and give a summary of the people or organisations that you represent.

We would welcome responses to the following questions set out in this consultation paper.

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?

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

Q7. [**For businesses**] Does your business involve SIM farms?

a) Yes

b) No

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

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-to-statutory-instruments-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)

Thank you for participating in this consultation.

Contact details and how to respond

Copies of this paper are being sent to:

- Devolved Administrations
- Ofcom (Office for Communications)
- National Crime Agency
- National Police Chiefs' Council
- City of London Police
- Crown Prosecution Service
- Serious Fraud Office
- His Majesty's Revenue and Customs
- His Majesty's Inspectorate of Constabulary and Fire & Rescue Services
- Association of Police and Crime Commissioners Organisations representing the interests of business and industry
- Signatories to the Telecommunication Fraud Sector Charter
- Telecommunications trade bodies, such as Mobile Ecosystem Forum, Mobile UK and GSM Association
- Non-Governmental Organisations (NGOs) with an interest in consumer rights and victim support
- Academics with an interest in fraud
- Parliamentarians

However, this list is not meant to be exhaustive or exclusive and responses are welcomed from anyone with an interest in or views on the subject covered by this paper.

Please send your response by 14 June 2023 at 17:00 via email at SIMfarmConsultation@homeoffice.gov.uk

Complaints or comments

If you have any complaints or comments about the consultation process you should contact the Home Office at the following address:

SIM farm Consultation
Economic Crime Directorate
Homeland Security Group
Home Office
6th Floor, Peel Building
2 Marsham Street
London
SW1P 4DF

Email: SIMfarmConsultation@homeoffice.gov.uk

Extra copies

Further paper copies of this consultation can be obtained from this address, and it is also available online at gov.uk

Alternative format versions of this publication can be requested from the Home Office at the above address.

Publication of response

A paper summarising the responses to this consultation will be published in following the end of the consultation. The response paper will be available online at gov.uk

Representative groups

Representative groups are asked to give a summary of the people and organisations they represent when they respond.

Privacy Notice

Confidentiality

Information provided in response to this consultation, including personal information, may be published or disclosed in accordance with the access to information regimes (these are primarily the Freedom of Information Act 2000 (FOIA), the Data Protection Act 2018 (DPA), the General Data Protection Regulation (GDPR) and the Environmental Information Regulations 2004).

If you want the information that you provide to be treated as confidential, please be aware that, under the FOIA, there is a statutory Code of Practice with which public authorities must comply and which deals, amongst other things, with obligations of confidence. In view of this it would be helpful if you could explain to us why you regard the information you have provided as confidential. If we receive a request for disclosure of the information we will take full account of your explanation, but we cannot give an assurance that confidentiality can be maintained in all circumstances. An automatic confidentiality disclaimer generated by your IT system will not, of itself, be regarded as binding on the Home Office.

The Home Office will process your personal data in accordance with the DPA and in the majority of circumstances, this will mean that your personal data will not be disclosed to third parties.

Privacy Notice

Your personal information, supplied for the purposes of this consultation, will be held and processed by the Home Office:

SIM farm Consultation
Economic Crime Directorate
Homeland Security Group
Home Office
6th Floor, Peel Building
2 Marsham Street
London
SW1P 4DF

The Home Office is the controller of this information. This also includes when it is collected or processed by third parties on our behalf.

Details of the Department's Data Protection Officer can be found at dpo@homeoffice.gov.uk Telephone: 020 7035 6999

Or write to:

Office of the DPO
Home Office

Peel Building
2 Marsham Street
London
SW1P 4DF

How and why the Department uses your information

The Home Office is only allowed to process your data where there is a lawful basis for doing so.

The Home Office fraud policy team will collate and analyse responses to better understand what SIM farms are, how they are used in the UK, the potential impact of the proposals on UK businesses and whether the proposals would help reduce smishing (mass scam SMS campaigns). The policy team will use the responses to form its final policy proposal and to develop legislation if necessary.

The Home Office may share your information with other organisations in the course of carrying out our functions, or to enable others to perform theirs.

More information about the ways in which the Home Office may use your personal information, including the purposes for which we use it, the legal basis, and who your information may be shared with can be found at Information rights privacy information notice - GOV.UK (www.gov.uk)

Storing your information

Your personal information will be held for as long as necessary for the purpose for which it is being processed and in line with departmental retention policy. More details of this policy can be found at What to keep: Home Office retention and disposal standards - GOV.UK (www.gov.uk)

Requesting access to your personal data

You have the right to request access to the personal information the Home Office holds about you. Details of how to make the request can be found at Personal information charter - Home Office - GOV.UK (www.gov.uk)

Other rights

In certain circumstances you have the right to:

1. object to and restrict the use of your personal information, or to ask to have your data deleted, or corrected.
2. (where you have explicitly consented to the use of your personal data and that is the lawful basis for processing) the right to withdraw your consent to the processing of your data and the right to data portability (where processing is carried out by automated means)

Questions or concerns about personal data

If you have any questions or concerns about the collection, use or disclosure of your personal information please contact the Home Office via info.access@homeoffice.gov.uk

Or write to us at:

Information Rights Team
Home Office
Lower Ground Floor, Seacole Building
2 Marsham Street
London
SW1P 4DF

You have the right to complain to the Information Commissioner's Office about the way the Home Office is handling your personal information. Details on how you do this can be found at Personal information charter - Home Office - GOV.UK (www.gov.uk)

Consultation principles

The principles that government departments and other public bodies should adopt for engaging stakeholders when developing policy and legislation are set out in the consultation principles.

https://www.gov.uk/government/publications/consultation-principles-guidance

E02907078
978-1-5286-4099-2