Home Office consultation on preventing the use of SIM farms for fraud

Response from Mobile UK

June 2023

About Mobile UK

1. Mobile UK is the trade association for the UK's mobile network operators (MNOs) – EE (a member of the BT Group), Three, Virgin Media O2 and Vodafone. Our goal is to realise the power of mobile and to improve the lives of our customers and the prosperity of the UK.

Introduction

2. Mobile UK welcomes the opportunity to respond to the Home Office's consultation on preventing the use of SIM farms.
3. Mobile UK's members invest heavily in time and resources to combat fraud both as individual operators and working together through the Communications Industry Crime Strategy Group and Mobile UK's Messaging Scams Group, which partners with the Information Commissioner, the National Cybersecurity Centre and Ofcom to share information and to assist with the suppression and prosecution of fraudulent activity online.
4. As such, Mobile UK supports the Home Office's strong desire to reduce the amount of scam and spam text messages being sent to the UK's consumers.

Response Summary

- Making it an offence to sell, own or use a SIM farm is a positive step, in that it sends a strong signal that the UK Government is prioritising this issue.
- It should mean they are more difficult to acquire and use and make it easier for law enforcement agencies to prosecute bad actors.
- However, it will not eradicate mass spam/scam SMS, which can still be sent from single SIM devices in large quantities, and current evidence suggests this is the most common way of doing so.
- The Government will need to consider broadening the definition of SIM farm to consider software or e-sim-enabled ways of achieving equivalent outcomes.
- There are also a few legitimate applications for multi-SIM devices where there are no cost-effective alternatives, and they should be accommodated in some way.
- More emphasis should be placed on prosecution of bad actors to have a significant impact on scam text messages.
- As the Home Office puts into effect the measures the proposals set out in the

Fraud Strategy, Mobile UK and its members look forward to working with them, regulators, and law enforcement to reduce the incidence of fraud and pursue and prosecute those who engage in it.

- The latter point is a key component of the proposed Project Inextended 2.

Mobile UK's Response to the Questions in the Call For Evidence:

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

5. Many mobile operator packages offer unlimited text messages as part of a package. However, such packages are not intended for 'bulk' use (and operators' terms and conditions make this clear), where, for example, an NHS dentist practice wishes to send out bulk check-up reminders to registered patients. While such an application would be a legitimate and lawful use of mass text messaging, such messages would (and should) be sent out through a wholesale route – the so-called 'application to person' [A2P] and this process does not rely on the presence of a SIM card.

6. It is unclear from the consultation document, though, whether the Government intends to include an 'e-SIM'1 within the definition of SIM farms.

7. Please see our response to Q2, where we argue that e-SIMs should potentially be included.

8. Mobile UK is inclined to support the proposal that a SIM farm should include any device capable of holding or using more than 4 SIMs. However, some iPhones, for example, can supposedly have space for as many as eight e-SIMs, and there may be arguments for allowing those that hold a few more, providing there is a legitimate commercial reason for doing so. Please see our response to Question 5.

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

9. As referenced in Q1, e-SIMs have an emerging presence on mobile networks worldwide. While they are not widely used in the UK at present, devices with many multiples of e-SIMs present a threat to the Government's objective of reducing scam messaging.

10. There may be little point in banning devices that can hold multiple physical SIMs without also restricting devices that contain many multiples of e-SIMs. To ensure effectiveness and prevent abuse, the definition of a SIM farm needs to be wider-ranging than the proposed government definition of a device containing more than four physical SIM cards. The role of Android SMS apps, virtual SIM hosting and e-SIM in facilitating SMS/voice fraud cannot be overlooked.

11. These comments are made in the context of devices with less than 4 SIMS remaining a significant threat, and current evidence suggests that single SIM devices are the most popular way of sending mass spam/scam text messages.

[1] https://www.gsma.com/esim/

12. The proscription of SIM farms will thus need to be just one of a range of future legislative measures to reduce the incidence of illegitimate mass SMS and online fraud.

13. It is interesting to note that the Information Commissioner has the power to pursue those that use mass SMS for unsolicited marketing. To the extent that it's within remit, they are employing such powers to pursue those with fraudulent intent.

14. There appears to be a gap whereby law enforcement can prosecute mass SMS, which is not unsolicited marketing but is yet of malicious intent (e.g. harvesting personal data such as passwords for use in an online crime).

Q3. What crimes are SIM farms used to facilitate?

15. It is well documented that SIM farms have been used to transmit very large numbers of text messages quickly. The evidence provided for the Economic Note by various police forces exemplifies this.

16. The content of the text messages has evolved. 5-10 years ago, the bulk of activity related to unsolicited marketing – for example, encouraging members of the public to use the sender's services for making PPI claims or accident compensation claims. The Government made earning a commission for generating leads for accident claims illegal, and PPI compensation ended. In more recent times, though (particularly as fraud has moved online), text messages have been used in various ways, particularly to harvest sensitive personal information such as dates of birth and passwords. This information can be used to access bank accounts and digital wallet accounts (e.g. Apple Pay or Google Pay).

17. The SIM farms generate large quantities of outgoing messages, so even if only a small proportion falls for the deception, the absolute number is still quite significant.

18. To combat this activity, mobile operators increasingly use SMS filters to block outgoing SMS and thus reduce the number of fraudulent text messages getting through to consumers.

19. In the last year, approximately 600m have been blocked this way. Moreover, the filters can implement rules (e.g., limiting the number of telephone numbers to which any SIM can send messages in a given time). This can severely impair the effectiveness and utility of SIM farms.

20. That said, filters are not perfect, as they have to be cautious about the risk of over-blocking and filtering out actual uses of SMS, such as the NHS sending out appointment reminders or banks sending out 'one-time-pass' codes. Moreover, the scammers are adept at sensing/interpreting any rules in place and working out ways of getting past the filter. It is a constant fight.

21. Thus, even though the SMS filters are having a positive impact on reducing the efficiency and effectiveness of SIM farms, we support the proposals.

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

22. The mobile operators' Spam Reporting Service database receives approximately 220k reports from the general public each week (some of which relate to voice calls too).

Consumers can report such messages by either forwarding to 7726 (SPAM on the alphanumeric handset) or responding 'yes' to a handset prompt 'this looks like spam, would you like to report it?' roughly 80-90% of reports into 7726 arise from such handset prompts. Virtually all SMS reported this way is either marketing, notifications or fraud. Many of the reported SMS is lawful/legitimate and have likely been reported because the customer thought them irritating or suspicious.

23. That said, current evidence provided to Mobile UK by one of the MNOs, suggests that the most common way of despatching such SMS comes from widely available single SIM devices.

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

24. Mobile UK understands there are some legitimate uses of devices with multiple SIMs, where connections are aggregated for applications such as live broadcasts by sports organisations and live entertainment providers. For example, this involves using multiple SIMs in a single device which connects TV cameras to do outside broadcasting. There are no cost-effective alternatives, we understand.

25. We would, therefore, not wish to see a complete ban on all single devices using more than four SIM cards, as certain businesses legitimately use a single device with more than four SIM cards.

26. Suppose these businesses are not able to move to other legitimate technology solutions because a practical cost-effective alternative does not exist. In that case, there should be a licensing regime (or exemption from proscription) overseen by Ofcom.

27. This would allow legitimate use cases to be able to continue or to be able to apply retrospectively for a licence in cases of genuinely legitimate use. If necessary, a controlled phase-out strategy could allow a sufficient period (minimum six months) to minimise disruption and cost for the organisation to migrate to a legitimate solution.

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

28. See Q5.

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?

29. By 'similar things', we take this to mean the capacity to send large numbers of messages in a very short time – something that can be achieved via 'bulk messaging' in the wholesale channel.

30. As mentioned in Q1, many legitimate reasons exist for sending messages in bulk (for example, a recruitment agency notifying job opportunities or housing associations housing vacancies).

31. Mobile operators' terms of service require that such bulk messaging be done through the wholesale A2P route.

32. Theoretically, it would be easy for scammers/spammers to switch to the bulk

wholesale channel. In practice, the aggregators (the intermediate service providers who handle bulk messaging for mobile operators) are contract bound to screen out spam and scam messaging traffic. It is, therefore, much more difficult for bad actors to use this channel, and only a relatively small proportion (perhaps between 10 and 20%) of reported SMS emanate from the wholesale channel. One mobile network has suggested ~10% of the scam messages they block have originated from the A2P channel.

33. Mobile UK supports that aggregators are coming within the scope of the Fraud Strategy so that the Home Office can explore further steps to eliminate unwanted traffic from the SMS communications routes.

34. The Government should also be aware that in light of the mobile operators' more effective blocking of fraudulent text messages with filters, fraudsters are migrating to over-the-top (OTT) applications that do not use the SMS channel but use WiFi or the mobile operators' internet access service, such as WhatsApp. These applications are outside the control of the mobile operators.

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

35. a) Yes
    b) No

36. There are legitimate reasons for having the ability to send large amounts of messages rapidly – for example, lawful, opted-in marketing campaigns; service messages to incoming overseas roamers; urgent communications (e.g. flood alerts); doctors' appointments, utility payment reminders; genuine fraud alerts. Extending a ban on other technologies and techniques must be undertaken with great care.

Q10. [For businesses] Does your business involve any of the items specified in Q8?

37. Yes. Mobile UK's members use mass messaging for many legitimate purposes: updating customers on network issues, regulatory compliance, bill notifications, reminders of contract renewal dates and a diverse range of customer communications.

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?

38. Yes – See Q8

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

39. Yes – See Q10

Q13. [For businesses] Does your business involve any of the items specified in Q11?

40. Yes – See Q10

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

41. [As discussed in Q1 and Q2, it is necessary to define whether the ban relates to devices with removable/physical SIM cards and/or devices with eSIMs and, if so, how many eSIMs are simultaneously active.] There is also a case for genuinely legitimate uses to be able to continue under a licence or an exemption.

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)?

42. Yes.

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

43. No views other than to say the fines should be gauged to have some deterrent impact.

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

44. Please see our response to Q5.

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

45. As discussed in our introductory comments, criminalising the sale and use of SIM farms will not necessarily prevent their use by bad actors entirely or stop them from sending out many thousands of SMS using single SIM devices. Still, the ban nonetheless strongly signals that law enforcement is taking the issue more seriously. The products should become less openly available on the internet.

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

a) Yes – please see our response to Q5
b) No
c) Don't know

Q20. Are there any other means to prevent criminals from abusing SIM farms that could also achieve the goal of protecting the public from mass text scams?

a) Yes
b) No

46. Mobile operators continually adapt the 'rules' on their SMS filters to counter the use of SIM farms. For example, they may restrict the number of different MSISDNs a customer can send SMS to, the timing, or some other metric indicating mass usage.

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?

47. Reducing the use of SIM farms should have a positive effect in that we would hope

fewer customers are sent unwanted text messages, but we cannot verify this. As far as we can detect, single SIM devices are currently responsible for the great majority of unsolicited mass text messages.

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 – for genuinely legitimate use cases.
b) No

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

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 – not specifically

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?

48. Please see our response to Q2.

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

49. With respect to mobile operators, Mobile UK agrees that the economic note reflects fairly the position. In particular, we agree that the costs of combating and dealing with the fallout from customers falling for fraud far exceed any possible revenue from purchasing SIM cards. The goal of the Home Office and the mobile operators to significantly reduce fraud are very much aligned.

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 – subject to appropriate consultation with stakeholders
b) No

50. There need to be clear parameters to exercise the Secretary of State's powers to add items to the list of banned technologies in the future. Our concerns about the definition of SIM farms would apply all the more to an open-ended power to define other technologies, the possession of which would be a strict liability offence. We

assume this would be the purpose of the new offence since an offence requiring proof of intent would be very similar to the existing offences in Sections 6 and 7 of the Fraud Act. We agree that conditions of evidence of use, stakeholder consultation and affirmative procedure are necessary and appropriate for adding items to the list of banned technologies.

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

51. Yes

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 – other than the intended impact on spammers/scammers

F. Call for Evidence

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

52. There are legitimate uses for multi-SIM approaches (please see our response to Q5), but Mobile UK is unaware of the scale.

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

53. It is difficult for a mobile operator to detect whether an actual SIM farm is in use, as each SIM (IMSI) and SIM slot (IMEI) has an identity on the network. It is thus difficult to detect whether spam/scam text messages are being sent from individual devices or an actual SIM farm. Also worth stating that some SIM farm devices can spoof IMEIs, thus effectively disguising themselves as other devices. Nonetheless, the sheer volume of spam SMS being blocked each day (c.600m to date) and the volume of reports received each day of spam SMS that have evaded the filters provide strong evidence that they are much in use. They are readily for sale on the internet, and mobile operators regularly detect large volumes of messages emanating from one cell in the network. This is all evidence that SIM farms are widely used to facilitate mass text messaging.

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

54. See previous replies.

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?

55. With respect to mobile operators, Mobile UK agrees that the economic note reflects fairly the position. In particular, we agree that the costs of combating and dealing with the fallout from customers being fraud far exceed any possible revenue gained from the purchase of SIM cards. The goal of the Home Office and the mobile operators to significantly reduce fraud are very much aligned.