Economic Note	Number: HOEN0026
Title of regulatory proposal	SIM Farm Regulation
Lead Department/Agency	Home Office
Expected date of implementation	Publication of the consultation – 3 May Legislation – when Parliamentary time allows
Origin	Domestic
Date	21/04/2023
Lead Departmental Contacts	Andrei.Skorobogatov@homeoffice.gov.uk Angeliki.Biliri@homeoffice.gov.uk
Departmental Assessment	GREEN

Rationale for intervention, objectives and intended effects

In the 12 months ending December 2022, there were an estimated 3.7 million incidents of fraud in England and Wales, making up more than 40 per cent of estimated crime. Criminals use technologies such as SIM Farms to target consumers via scam texts and calls. The Government believes that legislation is required to regulate technologies used by criminals to commit fraud. The strategic objective is to protect UK citizens from fraud enabled by technologies such as SIM farms via calls and texts and the intention is to reduce the level of fraud in the UK.

Policy options (including alternatives to regulation)

Option 1: Do nothing.

Option 2: Legislate to create a new criminal offence of manufacturing, importing, selling, possessing, and using technologies used for fraud in the UK. The offence will initially apply to SIM farms in the UK but may in the future be updated to include other similar technologies.

Costs and benefit summary

At this point evidence is not strong enough for a fully monetised appraisal and costs and benefits have been qualitatively assessed. Key costs are to businesses who manufacture, distribute or sell SIM farms who will have to absorb the costs of unsold stock and possibly lower revenue. The key benefit is a reduction in fraud.

Risks

There is a risk that the impact to business is higher than it has been possible to estimate, due to the limited evidence base, and it is likely that a change in regulation would not prevent criminals' ability to send mass SMS completely and may displace them to other methods.

Total Cost £m PV	Transition Cost £m	Cost to Business £m	Total Benefit £m PV
N/A	N/A	N/A	N/A
NPSV (£m)	**BNPV (£m)**	**EANDCB (£m)**	**BIT Score (£m)**
N/A	N/A	N/A	N/A
Price Base Year	**PV Base Year**	**Appraisal period**	**Transition period**
N/A	N/A	N/A	N/A

Departmental sign-off (*SCS*): Jemima Murray SRO Date: 27/04/2023

Chief Economist sign-off: Tim Laken SCS Date: 27/04/2023

Better Regulation Unit sign-off: Jon Bray BRU Date: 27/04/2023

Evidence Base

1. Background

1. The strategic objective of this measure is to reduce the volume and scale of fraudulent calls and texts reaching consumers in the UK, and the financial and emotional impact of the resulting frauds. Fraud represents a significant threat to the UK economy, consumers, and society, with nearly 3.7 million offences every year making up more than 40 per cent of all estimated crime[1].

2. In the year ending March 2022, Action Fraud, the fraud and cyber reporting service, received victim reports from individuals and businesses representing a financial loss of £4.2 billion[2]. It is likely that actual losses are much higher as only 14 per cent of fraud is reported[1]. Furthermore, wider societal costs are incurred in emotional harms to victims, victim support costs and preventative spend by business.

3. The proposals are in line with the commitment the Home Office made in the Fraud Strategy to block frauds from reaching individuals and businesses by making it as difficult as possible for criminals to operate at scale and without detection. They form part of wider work to secure telecommunications networks, including the Telecommunications Fraud Sector Charter[3] and Ofcom's strengthened rules and guidance[4] for providers to identify and block calls with 'spoofed' numbers.[5]

4. Home Office defines SIM farms as devices containing five or more Subscriber Identification Module (SIM) cards for one or more mobile networks, which enable the routing of calls or sending of text messages from fixed apparatus to mobile equipment by establishing a mobile-to-mobile call or data connection.

5. 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.

6. Therefore a device containing more than five SIM cards must be accessing a given network through multiple connections and therefore can be used in a different way to a device with four or fewer cards

7. According to the August 2022 'Ofcom Scams Survey[6], 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 an estimated 40.8 million adults in the UK. An estimated 700,000 followed the scammer's instructions, risking financial loss and significant emotional distress.

---

[1] Crime Survey for England and Wales: December 2022: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/crimeinenglandandwalesappendixtables

[2] Action Fraud. Fraud Crime Trends 2020-21. https://www.actionfraud.police.uk/data

[3] Fraud sector charter: telecommunications - GOV.UK (www.gov.uk) - https://www.gov.uk/government/publications/joint-fraud-taskforce-telecommunications-charter

[4] Statement: Improving the accuracy of Calling Line Identification (CLI) data – Ofcom - https://www.ofcom.org.uk/consultations-and-statements/category-2/improving-cli-data-accuracy

[5] The use of number 'spoofing', where the identity of the caller is disguised, is a frequent factor in scam calls.

[6] Ofcom Scams Survey: August 2022: https://www.ofcom.org.uk/__data/assets/pdf_file/0029/247493/ofcom-cli-and-scams-research-august-2022-slides.pdf

8. Texts are the most common form of suspicious message with more than six in 10 people (65 per cent of respondents) reporting that they had received suspicious texts. Reports of suspicious calls were lower but still significant. A total of 21 per cent of respondents reported suspicious live calls to their mobiles and 19 per cent to their landlines.

9. An unknown proportion of these messages come from technologies that enable criminals to operate at scale, such as SIM farms.

10. There is limited evidence that there are any legitimate use cases for SIM farms, and for all such cases alternative options likely exist. Therefore, the Home Office is consulting on proposals to regulate the manufacture, import, sale, hire and possession of SIM farms in the UK, as well as asking whether this ought to include other technologies without a known legitimate use.

11. The exact data on the link between SIM farms and mass scam texting is not currently known. The proposals in this consultation aim to make it more difficult for criminals to access and use technologies that enable them to target people at scale and undetected in the UK, like SIM farms. This is not currently possible under the existing Fraud Act 2006[7]. Home Office is launching a consultation on the proposals to ban the manufacturing, importing, selling, or offering it for sale, letting on hire or offering to let it on hire, and possessing or controlling of articles scheduled under the Fraud Act 2006. SIM farms are one such technology.

12. Similar capabilities are available on websites like iSpoof. iSpoof offered services that enabled those who signed up to the website 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[8].

13. Due to the limited evidence of legitimate and illegitimate usage, harm, scale and other factors, a call for evidence will be included as part of the consultation. The call for evidence will endeavour to gather information and data that will allow the Home Office to more accurately understand the volumes and impacts on businesses. The Home Office will then complete a more detailed appraisal to support the legislation.

Groups Affected

Businesses

- Businesses impacted by scam texts/calls
- Businesses who manufacture, distribute, or sell SIM farms
- Mobile Network Operators

Individuals

- Family, friends, and colleagues of perpetrators
- Family, friends, and colleagues of victims
- General public in the UK.
- Perpetrators

Public Sector

- Criminal Justice System (CJS)

[7] Fraud Act (2006) https://www.legislation.gov.uk/ukpga/2006/35/contents

[8] the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes.

- Crown Prosecution Service (CPS)
- Devolved Administrations (DA)
- Government departments
- HM Courts and Tribunal Services (HMCTS) (including equivalents in Scotland and Northern Ireland)
- Law Enforcement Agencies (LEAs) across the UK and members of these agencies.
- UK intelligence agencies and members of the UK intelligence agencies

2. The policy issue and rationale for government intervention

14. The Government has set out its ambition to tackle fraud in the Fraud Strategy, which includes significant effort to increase the law enforcement response to fraud, to empower victims to protect themselves and to work closely with industry and regulators to prevent the frauds in the first place. This work is a key part of this pillar, which also involves legislation to tackle online fraud and increased regulatory activity by Ofcom to tackle scam calls.

15. Scam texts are frequently traced back to SIM farms, which can house hundreds or thousands of SIM cards. Criminals use them to send tens of thousands of scam texts at once cheaply, quickly, and easily. They send out large volumes of Short Message Service (SMS) to "SMS phish"[9] for sensitive data, such as personal and bank details. SIM farms allow criminals to use all capabilities of SIM cards in bulk and at low cost.

16. Illegitimate uses of SIM farms include:

    a. Sending huge number of scam texts at low cost, with one police investigation discovering that five SIMs had sent over 900,000 messages in one SIM farm between April and October in one year.

    b. Scam call campaigns.

    c. Using data-only SIM cards to target victims on social media, for example by posting deliberately, misleading, false, or phishing messages online in bulk.

17. The mass texting and calling enabled by SIM farms can cause further problems such as network congestion, preventing legitimate calls and texts from going through. Industry experts[10] have suggested that 10-15 per cent of total mobile network traffic comes from SIM farms.

18. In one ongoing police investigation, one SIM farm has been found to be sending hundreds of thousands of texts a day. Banning the use of SIM farms will make it harder for criminals to send out scam texts on this kind of scale. Limiting the prevalence of fraudulent texts should reduce the number of people who become victims of fraud and the associated costs, including monetary losses and physical/emotional harms.

19. 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[11], but criminals are taking advantage of this to commit mass scam and phishing messages.

[9] SMS phishing also called 'smishing' is via SMS where the aim is to try and trick users into revealing personal information with messages that appear to be legitimate, such as alerts coming from banks.
[10] Industry expert in the telecoms industry who wishes to remain anonymous.
[11] A Global System for Mobile communication (GSM) Gateway is any equipment containing a SIM card which enables the routing of calls from fixed apparatus to mobile equipment by establishing a mobile to mobile call.

20. Government intervention is needed to solve the problem at source and target the means criminals use to send scam texts and scam calls, like SIM farms. This legislation intends to regulate the tools used by criminals to run mass fraud campaigns and provide law enforcement with the tools it needs to pursue criminals.

21. However, there are potential legitimate uses. SIM farms can be used in the Business-to-Customer SMS market, to reduce the costs of mass texting (such as marketing campaigns and automated appointment reminders). Many of the identified legitimate uses can be done with similar devices with less than five slots.

22. Any legislation will need to balance these legitimate uses against the objective of reducing criminals' ability to conduct fraud at scale and potentially the Public Sector's ability to send SMS alerts (although alternatives exist).

3. Policy objectives and intended effects

23. The aim of the proposals is to reduce the volume and scale of fraudulent messages reaching consumers via telecommunications means (that is, calls and texts). The proposals are likely to reduce the number of mass scam texts and calls sent to consumers. Home Office expect this to reduce the number of resulting frauds and the subsequent financial and emotional costs to victims.

24. Currently, a SIM Farm can be purchased online from online retailers and marketplaces, one platform was found to sell 16 slot SIM farms for £1,156. These are usually manufactured overseas and imported through legitimate retail channels. This legislation should make it impossible to purchase these devices in the UK through legitimate retailers.

25. The proposals are in line with the commitment the Home Office made in the Fraud Strategy to block frauds from reaching people and businesses by making it as difficult as possible for criminals to operate at scale and without detection. They form part of wider work to secure telecommunications networks, including the Telecommunications Fraud Sector Charter[12] and Ofcom's strengthened rules and guidance for providers to identify and block calls with 'spoofed' numbers[13].

26. This EN is supporting a consultation on the proposals to regulate SIM farms. The Home Office intends to ask consultees:

    a) What data do you have to demonstrate the scale of legitimate use of SIM farms and how many businesses currently use these devices legitimately?
    b) What data do you have to demonstrate the scale of illegitimate use of SIM farms and what is the current level of harm that they are causing to the general public in terms of losses, scam texts, emotional harm etc?
    c) What effects do you think a ban on SIM farms would have on both legitimate and illegitimate use?
    d) Are there any other technologies you think should be considered?

[12] Fraud sector charter: telecommunications - GOV.UK: https://www.gov.uk/government/publications/joint-fraud-taskforce-telecommunications-charter

[13] Guidance on the provision of Calling Line Identification facilities and other related services – Ofcom: https://www.ofcom.org.uk/phones-telecoms-and-internet/information-for-industry/telecoms-industry-guidance/calling-line-identification

Policy options considered, including alternatives to regulation

Option 1: (Do nothing)

27. Option 1 would entail no government intervention through changes to legislation, the technologies within scope would not be regulated and their status would remain unchanged. Costs and benefits for the other option assessed in this Economic Note are measured relative to the 'Do-nothing' position (which represents the counterfactual in this analysis).

28. Option 1 does not meet the Government's objectives.

Option 2

29. Ban the manufacture, import, sale, let or hire, possession and/or use of SIM farms.

30. The Government would bring forward legislation that would create an offence and list the proposed technologies, such as SIM farms and any other technologies identified in the consultation. 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.

31. The proposals would reduce criminals' access to technologies that allow them to target victims for fraud at large scale and low cost. Home Office anticipate that the application of the offence would lead to a reduction in fraud.

Non-regulatory options

32. Government, law enforcement and industry have already introduced non-regulatory measures to address mass smishing[14]. In 2019, Ofcom and UK Finance set up the DNO (Do Not Originate) list which records inbound-only telephone numbers that should not be used to call consumers, including those coming from SIM farms.

33. Additionally, in October 2021, the Government launched the Telecommunications Fraud Sector Charter[8], a voluntary code of nine actions for telecommunications providers. Actions include co-ordinated work to:

    a. Identify and implement techniques to block scam texts and calls.

    b. Work closely with law enforcement and the financial industry to disrupt frauds in progress and prosecute offenders.

    c. Engage with consumer and victim support groups to improve support to victims of telecoms fraud.

34. Industry initiatives have also looked to protect consumers, legitimate businesses and organisations falling victim to text messaging scams, through systems that verify the message header of an SMS.

35. Despite these measures, evidence suggests that the volume and scale of fraudulent messages reaching consumers via telecommunications remain high. Criminals currently do not face any barriers in terms of procuring SIM farms.

[14] The fraudulent practice of sending text messages purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords or credit card numbers.

36. The government is consulting to better understand the possible impacts of Option 2. When considering whether to legislate, the full balance of impacts and possible costs and benefits will be considered.

Appraisal

37. Due to a lack of sufficient evidence, there remain uncertainties in relation to the impact of the proposals to businesses and the costs associated with introducing and implementing the ban.

38. The consultation document will include a call for evidence, to collect information and data that may allow for more accurate estimates of the volumes and impacts on businesses affected to be made.

General assumptions and data

39. While efforts have been made to understand the costs and benefits to all affected groups, all costs and benefits are non-monetised. Where possible figures are provided to give a sense of scale and rely on the current best assumptions, rather than comprehensive evidence. At this point evidence is not strong enough for a fully monetised appraisal and therefore costs and benefits have been qualitatively assessed.

40. Home Office have used available data to develop the evidence base for this economic note and will endeavour to use information gathered through the consultation to strengthen and update the analysis before a final IA is published.

Summary of costs and benefits by groups affected:

Group	Costs	Benefits
General Public	The general public are not expected to incur any direct costs as a result of regulating SIM farms.	The ban on SIM farms would reduce the levels of scam texts that consumers receive, which is expected to reduce the volumes of fraud victims and loses. The reduction of SIM farms on mobile networks would lead to a better consumer experience due to less network congestion.
Public Sector	Familiarisation costs for police and Border Force staff.	
Mobile Network Operators (MNOs)	MNOs currently receive revenue from the large volumes of SIM cards that are purchased and used by criminals in SIM farms. A ban on SIM farms would therefore lead to lower MNO revenues.	MNOs incur extra costs currently as they are required to invest in increasing infrastructure capacity, as SIM farms cause slower network access and can lead to signal masts malfunctioning. The cost of manufacturing and distributing SIM cards which are being switched off within 30 minutes can represent a loss to MNOs. MNOs also incur costs detecting and deactivating SIM cards used in SIM farms.
Legitimate users	Businesses who are currently legitimately using these devices would have to stop using them and fund the cost of switching to an alternative technology.	
Retailers	Online retailers and marketplaces who are selling these devices would incur compliance costs and lost revenues in the future, due to the ban and would be required to absorb the costs of any unsold stock.	
Distributors and Manufacturers	Businesses who are currently distributing or manufacturing these devices in the UK, would be required to cease their distribution and absorb the costs of any unsold stock and machinery. No evidence of UK-based manufacturers has been found.	

Costs

Set-up costs

Private Sector

41. Businesses who manufacture, distribute, or sell SIM farms would be required to cease their sale, distribution, and production, and absorb the costs of any unsold stock.

42. Businesses who currently legitimately use SIM farms would have to shut them down and identify alternative technologies to use. Without further evidence on the scale of usage and use-cases, further assessment of this cost has not been possible.

43. Criminals use SIM farms by inserting high volumes of SIM cards into them, which are purchased in bulk. The loss of these SIM farms would harm MNO revenue as fewer SIM cards are sold. However, as detailed in the benefits, and evidenced by the activities MNOs take to shut down SIM farms, it is expected that this is outweighed by their cost savings.

Public Sector

44. Public sector familiarisation costs are expected. Constables and senior police officers would be expected to familiarise themselves with the new legislation. This is expected to be via an email or letter that would notify the reader of the changes in legislation and amendments to internal guidance documents.

45. Border Force staff would also be expected to familiarise themselves with the legislation, in order to stop SIM farms entering the UK. This is expected to be via an email or letter that would notify the reader of the changes in legislation and amendments to internal guidance documents.

Ongoing and total costs (Private and Public)

Private Sector

46. Online retailers and marketplaces who currently sell these devices would incur ongoing costs, in ensuring that SIM farms aren't advertised or offered for sale on their platforms going forwards, and they are complying with the new legislation.

47. Businesses which sell SIM farms on their platforms may see a reduction in revenue as they can no longer sell these devices.

48. It is possible that the alternative solutions for businesses who legitimately use SIM farms would be more expensive. This would incur an ongoing cost equal to the difference.

49. Further assessment of private sector costs has not been possible as Home Office lacks information on the market for SIM farms.

Benefits

50. Due to a lack of data on the prevalence of SIM farms in the UK, this economic note will provide only qualitative assessment of the possible benefits of the proposed legislation.

Set-up benefits

51. No set-up benefits are expected.

Ongoing and total benefits

Private sector

52. SIM farms can slow down access to the network for customers, including sometimes causing signal masts to malfunction. This might require the operators to invest in infrastructure upgrades to increase capacity. Operators will either pass the cost on to customers by increasing their prices or absorb the cost of upgrading at their own expense. For one operator, an investment of £0.25 million was made to increase capacity in a cell area, but it was subsequently discovered that 70-80 per cent of the traffic there was driven by SIM farms, rather than legitimate use. The legislation would benefit operators by reducing the risk of SIM farms placing an excessive burden on cell areas.

53. The costs to MNOs of SIM farms such as network congestion, and short-lived SIM cards lead to incentives to identify and block SIM cards used in SIM farms. One operator (BT/EE) has reportedly blocked 30,000 SIM cards since August 2021. A reduced need to block these SIM cards is expected to reduce MNO operating costs.

54. The cost of manufacturing and distributing SIM cards is normally balanced by the consumer purchasing a monthly contract or pay-as-you-go minutes/SMS. SIM farms require large numbers of SIM cards, which are switched out, blocked and discarded frequently, sometimes within 30 minutes of activation. This can represent a loss to operators and the banning of SIM farms is expected to reduce this cost.

55. Evidenced by the activities MNOs take to shut down SIM farms, it is expected that the benefits listed above would outweigh the revenue losses explained in the private sector costs section.

General public

56. Criminals can use SIM farms to send tens of thousands of scam texts at once. A ban on SIM farms would make it more difficult to send high volumes of scam messages and likely reduce the volume of scam texts consumers receive.

57. This is expected to reduce the level of fraud, and the corresponding socio-economic harms. Reduced levels of fraud experienced by the public would reduce the levels of emotional harm victims suffer, victim support costs and financial losses.

58. If SIM farms are causing network congestion, consumers experience reduced network connectivity when trying to send legitimate calls and texts on a network. Banning SIM farms would reduce the levels of network congestion and provide a better service to consumers on mobile networks when trying to make legitimate calls and texts.

Value for money metrics

SaMBA

59. It is expected that there would be very little impact on small and micro-businesses (SMBs), since it has not been possible to identify any legitimate uses of these devices by SMBs. Some SMBs may potentially have bought SIM farms but the scale of this is unknown, which is expected to be revealed via the call for evidence.

60. For these businesses, there would be an upfront cost to replace this with an alternative device and this cost may have a greater relative financial impact on small and micro businesses. It is unclear, however, how many businesses this would apply to, and given the higher cost of SIM farms it is unlikely this would be the case.

6. Risks

61. The proposed measures do not appear to pose any large risks; however, the following have been identified as potential problems:

    a. There is a risk that the impact to business would be higher than it has been possible to estimate, due to the limited evidence base. The consultation process aims to bring this information out via the consultees, and therefore mitigate the potential risk of bringing in legislation without fully understanding the cost to business.

    b. The proposed ban would limit criminals' ability to send out mass SMS, however it would not prevent them from doing so completely. It may displace criminals to other methods of committing fraud. The Home Office is aware of several potential ways around the ban which would still enable SMS to be sent out on a large scale.

    c. Since alternative methods exist, this policy does not expect to completely prevent criminal mass SMS but aims to frustrate criminals' abilities to do so.

    d. These alternative methods are often more expensive, require more technological knowledge, or are less efficient. The ban can therefore still be expected to reduce the number of scam texts being sent.

7. Implementation, monitoring and evaluation

62. The Home Office will develop a monitoring and evaluation plan once the legislation and operational-delivery have been finalised.

Specific Impact Test Checklist

Mandatory specific impact test - Statutory Equalities Duties	Complete
Statutory Equalities Duties The public sector equality duty requires public bodies to have due regard to the need to eliminate discrimination, advance equality of opportunity, and foster good relations in the course of developing policies and delivering services. The primary objective of the proposals is to make it more difficult for criminals to access technologies that allow them to carry out fraud at scale and at low cost. The policy will effectively add barriers for fraudsters trying to contact potential victims. There is no evidence of direct discrimination due to the policy proposals. Overall, Home Office believes the benefits of these policies outweigh any potential risks. By placing more emphasis on shutting down opportunities for fraudsters, the burden of fraud prevention is reduced for the public. This allows all, including those in protected characteristic groups, to engage in everyday communications more safely and without exclusion. The proposals cover all communities, demographics and protected characteristics equally. They aim to stop fraudsters from trying to contact their potential victims, thus increasing protection for all potential victims, irrespective of the existence or lack of protected characteristics. Additionally, the proposals place the burden of responsibility on companies to stop buying, selling, possessing and using SIM farms; and law enforcement to identify, stop and prevent these activities. It is likely to reduce the burden on elderly, less technologically educated people to educate themselves on telecommunications safety and will increase the opportunities of all protected characteristics to use the telecommunications network, safer from fraud.	**Yes**