Impact Assessment

Title:	Crime and Policing Bill 2025 – Measures Impacting on Business
Type of measure:	Primary Legislation
Department or agency:	Home Office
IA number:	HO IA 1010
RPC reference number:	RPC-HO-24018-OA (1)
Contact for enquiries:	CrimeandPolicingBillTeam@homeoffice.gov.uk
Date:	2 December 2025

1. Summary of proposal

Proposal 1: Reform the Identification Doctrine

1. Criminal activity can be enabled and perpetuated by corporations, as it is by individuals. The objective of this proposal is to legislate for a legal test to attribute acts of criminal conduct to corporations[1], partnerships[2] or corporate bodies[3], as entities in their own right.
2. The identification doctrine is the legal test that decides whether the actions and mind of a natural person can be regarded as those of a legal person. Prosecuting authorities generally seek to identify someone with the status, for example, of a director, who has committed the criminal offence and there would be reasonable grounds for such individuals to have the necessary authority to constitute the directing mind and will of

[1] 'Corporation' includes a number of legal structures. Two main characteristics of corporations are that they are recognised as a separate legal entity from their owners and that shareholders are not personally liable for any debts or claims against the business.

[2] A partnership is the merger of several legal entities that pursue a common goal. These legal entities can be natural persons, legal bodies (usually corporations), or other partnerships. Under this legislation, a partnership will be defined as a partnership within the meaning of the Partnership Act 1890; (b) a limited partnership registered under the Limited Partnerships Act 1907; (c) a firm or other entity of a similar character to one within paragraph (a) or (b) formed under the law of a country or territory outside the United Kingdom.

[3] Corporate bodies are separate entities under the law to the natural persons that are associated with it (employees or similar), enabling a chain of attribution from one to another.

the organisation. This legal principle has developed over time in case law since *Tesco v Nattrass* in 1971.[4]

3. The current common law for holding organisations criminally responsible in recent years has raised concern that parts of the law are not fit for purpose. This has hindered the successful prosecution of corporations. In 2023, the previous government introduced the Economic Crime and Corporate Transparency Act 2023 (ECCT Act 2023).[5] This enabled a corporate body or partnership to be held criminally liable where a senior manager commits a specified economic crime offence while acting with the actual or apparent authority granted by the organisation. Due to the limited scope of the ECCT Act 2023, the identification doctrine provision was only applicable to economic crimes. However, the previous government committed to applying the identification doctrine reforms to all crimes, as soon as Parliamentary time allowed.

4. This measure will apply the same change in legislation introduced in ECCT Act 2023 to all offences, holding a corporation or partnership liable for a criminal offence if it is committed by a senior manager. This provision (as with that in ECCT Act 2023) does not replace or amend the common law identification doctrine but provides a new statutory route to corporate liability for all offences. In doing so, it repeals and replaces the provisions in ECCT Act 2023.

Proposal 2: Suspension of Internet Protocol Addresses and Internet Domain Names

5. Internet Protocol (IP) addresses and domain names are used by criminals to facilitate a range of criminal offences including phishing, fraud consumer scams, child sexual abuse material, and dissemination of malware. Members of the public may access these IP addresses and domain names unknowingly and, in some cases, become victims of serious crimes.

6. At present there is no legal power available to law enforcement (LE) and investigative agencies to require industry to take action to suspend these IP addresses and domain names. LE and investigative agencies have to rely on voluntary arrangements with industry to do so. In the majority of cases in the domestic sphere, voluntary arrangements are successful. However, most registries and registrars are situated in foreign jurisdictions and require a formal request, such as court order, before they will take action.

7. This measure will be used to allow agencies to formally request action by organisations outside the UK. It will also allow them to formally request action in the small number of domestic cases where voluntary arrangements will not work.

8. The power will be available to the National Crime Agency (NCA), Police Forces, HM Revenue and Customs (HMRC), Financial Conduct Authority (FCA), and the Gambling Commission.

[4] Tesco Supermarkets Ltd. v. Nattrass: https://www.uniset.ca/other/cs2/1972AC153.html

[5] Economic Crime and Corporate Transparency Act 2023: https://www.legislation.gov.uk/ukpga/2023/56

Proposal 3: Ban the supply or possession of devices known as 'SIM farms' in the UK

9. Legislate to introduce two new criminal offences criminalising the supply or possession of a SIM farm[6], unless there is a good reason, or adequate due diligence has been undertaken.

10. The maximum penalty for the offence is an unlimited fine in England and Wales and a level 5 fine (currently £5,000) in Northern Ireland and Scotland.

11. The measure also allows the extension of the ban to other technologies that are at significant risk of being exploited by criminals to commit fraud facilitated by electronic communications. The Secretary of State will be able to specify such technologies in the future, subject to a high level of scrutiny and checks.

2. Strategic case for proposed regulation

Proposal 1: Reform the Identification Doctrine

12. The objective for reforming the identification doctrine is to clarify the common law model to increase prosecutions of corporations for all criminal offences committed by senior management.

13. In recent years, concern has been expressed that the identification doctrine devised in the 1970s does not adequately deal with misconduct carried out by and on behalf of modern-day corporations. This is because:

    a. It is too narrow – only a small number of persons are considered the "directing mind and will" of a corporation.

    b. It does not reflect the reality of decision-making in complex corporations – decision-making can be dispersed across multiple directing minds leading different areas of a corporation.

    c. It makes it too difficult to convict corporations for offences committed for their benefit – corporates are gaining financially from economic crimes and should be prosecuted accordingly.

    d. It is unfair between small and large companies – the "directing mind and will" is easier to identify in a small organisation that may have one to two directors controlling the business.

    e. It does not always bring certainty – the current law has developed through the courts and has not got legislation underpinning it.

    f. It does not encourage good corporate governance and may deter it – a corporate could escape liability under the common law by making their governance artificially complex so it is difficult to determine a singular "directing mind and will".

14. In 2023, the previous government introduced reform of the identification doctrine for economic crimes in ECCT Act 2023. The reform placed the identification doctrine on a statutory footing (for economic crimes), providing certainty that senior managers are in scope to better capture large ownership structures. Under the statutory identification

[6] SIM farms are electronic devices which can hold sometimes hundreds of SIM cards that can then be used to send out thousands of scam texts and calls in seconds.

doctrine, the corporation will be prosecuted for crimes committed by a senior manager, if acting in the authority granted by the corporation, as if they were the senior manager themselves. However, the identification doctrine developed in current common law applies to all crimes, not only economic crimes, so a wider reform is required to apply to all criminal offences in the UK. Examples of offences that are in scope include those committed by an individual through the authority granted by an organisation such as trading offences, environmental offences and animal cruelty offences. The reform will help to address instances of failed prosecutions relating to these offences due to limitations under the current common law model.

15. For instance, in the case of R v St Regis Paper Company Ltd 2011, the prosecution failed to impose criminal liability on a company based on the dishonest intentions of its technical manager for an offence of making false entries in a record required for environmental control.[7] This case exemplifies that further government intervention is required to place the identification doctrine for all crimes, not just economic crimes, on a statutory footing, to ensure cases are successfully prosecuted.

16. The rationale for this policy is to address the disparity in being able to criminally prosecute small and large organisations: the current corporate criminal liability model makes it difficult for prosecutors to successfully pinpoint the directing mind and will of a large organisation with multiple directing minds across different areas of the business.

17. By contrast, directors in a smaller organisation are closer to the level at which misconduct took place (for example, by explicitly or implicitly authorising the commission of a criminal offence) and more likely to have the knowledge needed to satisfy the directing mind and will test, creating an equity failure.

18. The government is of the view that a rule which impacts disproportionately on smaller companies but fails to deal satisfactorily with similar conduct in larger firms is unfair. The reforms will address this equity failure and increase confidence in the criminal law.

19. The reform of the identification doctrine is not intended to add to the legal and regulatory burdens which are already imposed on businesses. Breaches of existing obligations would be more effectively sanctioned under the criminal law, resulting in a better-functioning Criminal Justice System (CJS).

20. Without the reform, the UK could fall behind international standards in the prosecution of organisations criminal activity. In particular, the UK may lack an ability to bring proceedings in high-profile cross-border criminal cases in support of partner agencies such as the US Department of Justice.

21. The ability to capture data on corporate convictions for non-economic crime offences using an attribution model from a natural person to a corporate is difficult. The model for attribution from a natural person to corporation has previously only existed in common law (since Tesco v Nattrass in 1971), which lacks legal certainty, meaning that there has been a general lack of awareness and confidence in applying the identification doctrine broadly. There has been a greater possibility that cases did not proceed at investigation stage (and prosecution stage) against corporate entities due to the challenges under the common law.

---

[7] St Regis Paper Company Ltd v R. [2011] EWCA Crim 2527 (04 November 2011): https://www.bailii.org/ew/cases/EWCA/Crim/2011/2527.html

22. This reform will create one avenue in law for prosecuting any corporation for a criminal offence if the offence is committed by their senior management. This applies to any law in the UK meaning that it is extremely wide. It is challenging to collect data on potential cases that the identification doctrine could apply to. Collecting data across all areas of criminal law is also costly as it requires consultation with users of any law in the UK.

23. This means that any collected data is likely to contain high levels of inaccuracy due to the breadth of potential cases it could apply to. Additionally, such data could not be future proofed as new laws are created regularly that could be in scope of the identification doctrine.

Proposal 2: Suspension of Internet Protocol Addresses and Internet Domain Names

24. The overriding strategic objective of the provision is to reduce a range of crimes such as computer misuse offences, phishing, fraud, Child Sexual Abuse Materials, and dissemination of malware. This includes crime in the UK, and crime originating abroad which has an impact in the UK.

25. The volume of cyber crime in the UK is extensive and can have huge effects on victims. In the year ending June 2024, there were an estimated 952,000 incidents of computer misuse experienced by adults aged 16 years and over in England and Wales[8].

26. In the year to March 2024, 24 per cent (34,000) of computer virus incidents in England and Wales (139,000) involved loss of money or property and in 47 per cent of computer misuse incidents in England and Wales the victim was emotionally affected in some way in the year to March 2023.

27. In addition, computer misuse offences often facilitate more serious crimes such as fraud, consumer scams and child sexual abuse material, providing LE agencies with a power to mandate the suspension of IP and domain names can help address this[9].

28. Criminal actors can use IP addresses and/or domain names to carry out crime and manage remote systems such as crime sites or botnets. A botnet is a network of infected systems, typically being controlled without the knowledge of victims, whose computers are being controlled as a platform to further promulgate malicious activity (for example, sending spam, acquiring data, proxying criminal communications or carrying out denial of service attacks).

29. Such botnets can operate at significant scale. In a recent case, one botnet infected an estimated 1.5 million systems worldwide with malware[10].

30. When domain names and devices associated with IP addresses are being used to conduct criminal activities, LE need to be able to act to block access to those IP addresses and domain names by suspending them. By equipping LE and certain investigatory agencies with the necessary powers to suspend access when the IP

---

8 Crime in England and Wales: Appendix tables - Office for National Statistics (ons.gov.uk): https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/crimeinenglandandwalesappendixtables

9 Crime in England and Wales: Appendix tables - Office for National Statistics (ons.gov.uk): https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/crimeinenglandandwalesappendixtables

10 Office of Public Affairs | Criminal Marketplace Disrupted in International Cyber Operation | United States Department of Justice: https://www.justice.gov/opa/pr/criminal-marketplace-disrupted-international-cyber-operation

address and/or domain names are being used for serious crime, the government can prevent harm to victims of cyber crime and other offences that are facilitated through computer misuse.

31. By suspending an IP address it's possible to sever the link between the domain name and its ultimate destination, which disrupts the criminal behaviour as a device cannot be reached. This change can be actioned by both the registry and registrar associated with the domain.

32. Action by LE against domains and IP addresses aims to disrupt or stop criminal activity that is causing harm in the UK rather than to investigate possible offences with a view to bringing criminal charges. The National Cyber Security Centre (NCSC) 2024 annual report reports that 2.2 million cyber-enabled commodity campaigns removed (up from 1.8 million in the previous year)[11]. The National Police Chiefs' Council (NPCC) said that they had had 458 requests rejected in the last year.

33. The ability of LE agencies to suspend domains and/or IP addresses is already available in most developed jurisdictions such as the United States of America but is not available to UK LE agencies. Were a power to be available here, it would enable domestic LE agencies to break the communication link between criminal and victim computers.

34. The NCA provided the below case study which exemplifies where not having a legal means of suspending IP addresses or domains reduces the effectiveness of UK LE operations:

35. Redline Stealer is a malware variant that harvests information from browsers such as saved credentials, autocomplete data, and credit card information. In October 2024, a Europol-led operation was used to co-ordinate the international takedown of important infrastructure relating to Redline Stealer malware. As part of this operation, the NCA were provided with information on multiple Redline servers based in the UK. The NCA were able to suspend the majority of UK based redline servers through voluntary co-operation from hosting providers. However, in one instance, a UK registered hosting provider was unresponsive and did not respond to a suspension request. This reduced the effectiveness of the co-ordinated takedown and left UK citizens vulnerable to further victimisation.

Domestic position

36. LE currently utilise voluntary arrangements with industry to suspend domain names. There are good relationships with the main UK registry, Nominet (who manage the ".UK" country code) and registrars (who are closer to the customer, and work as resellers) operating in the UK. The registry and registrars voluntarily suspend access in most instances when LE make a request since facilitating crime is generally against the terms and conditions of domain registration. These voluntary arrangements ensure domains are suspended and it is the strong intention that these voluntary arrangements continue as the first port of call, with a court order only being used in exceptional circumstances (for instance, when a provider refuses to voluntarily suspend the domain name).

Overseas

[11] cyber-enabled commodity campaigns removed (up from 1.8 million last year)

37. While the consensual domestic arrangements work well, they are limited to the small portion of the internet that is located in the UK. The overwhelming majority of internet infrastructure is situated in foreign jurisdictions. In these cases, it is more difficult to take these IP addresses and domain names down as having consensual relationships with all international registries and registrars is not practical. Overseas entities such as Interpol do not always recognise informal requests without court orders from LE and it is not practical to have consensual relationships with international providers in the same way that LE has domestically.

38. Many relevant organisations internationally require court orders before they will suspend domain names and IP addresses. The NCA estimate that there are between 10 to 40 cases (where there would be multiple IPs and domains suspended as part of the investigation) annually they are not able to act on in foreign jurisdictions due to the lack of a legal power. These are often high harm, high impact cases which have a significant impact on UK citizens and businesses, and which require partnership with major allies.

39. Whilst a UK court order cannot compel foreign entities to act upon it, and there will be some jurisdictions which would never cooperate, having a process to obtain a court order to be served overseas would improve current arrangements with likeminded countries. Governance processes at an international level are also helpful in supporting international court orders being served and actioned. Gaining a court order will likely be the first port of call for suspending IP addresses and domain names hosted overseas. The Home Office has not been able to source appropriate data from foreign jurisdictions to allow successful international comparisons. Where other countries have different legal systems and approaches to addressing cyber crime this limits the effectiveness of comparison.

Consultation

40. A public consultation[12] took place on the power from 7 February 2023 to 6 April 2023 which sought views on support for the power, any barriers to implementation and evidence of impact of the power not being implemented. A total of 43 responses to the consultation paper were received. Of these, approximately half of responses were from individual organisations (including charities, trade associations and technology companies).

41. Several police forces also responded to the consultation as well as various working groups and peer groups. In addition to this, a small number of both individual and academic responses were received. The then government response to the consultation was published in November 2023. There was broad support for a new power to allow LE agencies such as the NCA, the police, and other agencies with investigatory powers to suspend domains and IP addresses.

42. The consultation asked respondents *'How can voluntary agreements, which are the preferred route for take downs, be protected?'*. Over a third of respondents who answered this question, thought that voluntary arrangements should be used initially and that mandatory requests should only be used when voluntary arrangements are

[12] Review of the Computer Misuse Act 1990 - Analysis of Consultation Responses: https://assets.publishing.service.gov.uk/media/655390ca50475b000dc5b5b9/CMA_Consultation_Response.pdf

either not available or have failed. One respondent argued that a proper oversight and appeals process may also help to protect voluntary agreements.

43. Despite this, several respondents expressed concerns that mandatory requests may undermine voluntary agreements because organisations may insist that, where a statutory court-based route exists, it should take primacy and organisations would only respond to suspensions under the statutory arrangements. The IP and domain power has been designed to take this into account. One of the conditions that a judge must be satisfied is met to grant the order is that there's no alternative route to the same end (for example, a voluntary arrangement with the provider would seriously prejudice the prevention of crime).

44. The consultation asked respondents '*what will a statutory power enabling the seizure of domain name and IP addresses allow that voluntary arrangements do not currently allow?'.* In response to this, the majority of the respondents agreed that a statutory power would provide the opportunity to compel take-down in the event of non-compliance with a voluntary arrangement. Respondents told us that they cannot rely on voluntary agreements internationally as many jurisdictions require court orders before they will take action.

45. Multiple respondents also argued that this power may assist the UK to work more effectively with overseas LE agencies by bringing the UK's standards in-line with international precedent, allowing for the use of Mutual Legal Assistance Treaty requests (MLATs) and other international requests.

Proposal 3: Ban the supply or possession of devices known as 'SIM farms' in the UK

46. Fraud is the most common crime type in the UK making up approximately 43 per cent of all CSEW (Crime Survey of England and Wales estimated crime). In the year ending December 2024, there were an estimated 4.1 million incidents of fraud[13].

47. In the year ending March 2022, Action Fraud, the fraud and cyber crime reporting service, received victim reports from individuals and businesses representing a financial loss of £4.2 billion[14]. It is likely that actual losses are much higher given the historic underreporting of fraud.

48. Wider societal costs are incurred in emotional harms to victims, victim support costs and preventative spend by business. The Home Office estimates that the total cost to society of fraud against individuals in England and Wales was at least £6.8 billion in 2019/20[15]. The Economic Crime Survey reports that in 2020 around one in five businesses had been a victim of fraud in the previous three years (18 per cent)[16] .

[13] Crime in England and Wales: Appendix tables - Office for National Statistics: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/crimeinenglandandwalesappendixtables

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

[15] Fraud Strategy: stopping scams and protecting the public (accessible) - GOV.UK: https://www.gov.uk/government/publications/fraud-strategy/fraud-strategy-stopping-scams-and-protecting-the-public#the-harm-fraud-causes

[16] Economic Crime Survey 2020 - GOV.UK (www.gov.uk): https://www.gov.uk/government/publications/economic-crime-survey2020#:~:text=The%20Economic%20Crime%20Survey%20(ECS,%2C%20and%20information%20and%20communication).

49. Criminals use technologies such as SIM farms to target consumers via scam texts and calls. A SIM farm is a device which is capable of using five or more physical SIM cards to make phone calls or send short message service (SMS) text messages. SIM farms are used by criminals to send out thousands of scam texts to defraud the UK public of millions of pounds. They are also used to run scam call campaigns and to mask communications data when making calls or texts, making investigations significantly more difficult.

50. There are substantively only four mobile operators in the UK, with all other providers piggybacking off their services. Devices with more than four SIM card slots are accessing at least one network more than once concurrently and are being used differently to most normal connections. Whilst this could be for a legitimate purpose such as to improve the quality of a data connection, this is frequently used by fraudsters and organised criminals to send out large volumes of texts or calls.

51. There is no publicly available and reliable market size data for the legitimate businesses using SIM farms due to the absence of transparent data. The market is not widely publicised and there are no reports or studies detailing its size and revenue. The government issued a call for evidence as part of its public consultation which sought data or evidence to demonstrate the scale of legitimate use of SIM farms. The call for evidence returned limited information – all information received has been included in the present IA.

52. Given the small scope of legitimate use of this technology in this way, it is clear there is a market for this technology that is solely used for fraud and criminal activity. This legislation will allow the government to separate the legitimate market from the criminal use of SIM farms. According to Ofcom, in the period November 2024 to February 2025, 64 per cent of people in the UK said they had received a suspicious message, in the form of either a text, recorded message or live voice call to a landline, mobile or an app message. This represents an estimated 35.7 million adults in the UK[17]. Texts are the most common form of suspicious message with 54 per cent of mobile users reporting that they had received suspicious texts. A further 21 per cent of respondents reported they had received a suspicious app-based message[18].

53. One per cent of respondents who had received a suspicious text/app message/live call said they clicked on the link and then did as instructed by the message/ person. This equates to approximately 558 thousand adults aged 16 years and over in the UK. Reports of suspicious calls were lower but still significant: 32 per cent of respondents reported suspicious calls to their landline and 19 per cent to their mobiles[19].

54. The proposals 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[20].

55. Sending scam emails, texts, or phone calls to trick victims ("phishing") is illegal under the Fraud Act 2006 or the common law in Scotland. However, this does not prevent criminals acquiring equipment such as SIM farms with the aim of conducting fraud. The

[17] Ofcom Scams Survey 2025: https://www.ofcom.org.uk/about-ofcom/our-research/statistical-release-calendar-2025
[18] Ofcom Scams Survey 2025: https://www.ofcom.org.uk/about-ofcom/our-research/statistical-release-calendar-2025
[19] Ofcom Scams Survey, March 2025 https://www.ofcom.org.uk/about-ofcom/our-research/statistical-release-calendar-2025
[20] Fraud Act 2006 https://www.legislation.gov.uk/ukpga/2006/35/contents

government believes that legislation is required to regulate technologies used by criminals to commit fraud and prevent frauds from reaching individuals and businesses.

56. This intervention is required to make it as difficult as possible for criminals to operate at scale and without detection. The proposals are in line with the government's commitment to address the full range of fraud threats, including online, public sector and serious fraud.

57. SIM farms increase the costs to firms of scam-prevention, by increasing the prevalence of scam communications. This measure may reduce costs to Mobile Network Operators (MNOs) by reducing the quantity of scam messages they need to protect their customers from.

Public consultation

58. On 3 May 2023, the Home Office launched a consultation on proposals to ban SIM farms in the UK and sought views on their definition and potential legitimate uses[21]. The consultation also sought views on other technologies used by fraudsters and asked whether the Home Secretary ought to be able to update the list of banned articles in the future.

59. Responses to the consultation supported the proposed approach to addressing the issue of SIM farm equipment being used to perpetrate fraud. Respondents agreed that the ban would raise the barriers to entry for those engaging in illegal activities, making it more difficult for them to obtain and exploit SIM farms for fraud. However, they raised concerns that the wide definition of SIM farms, as set out in the consultation, risked affecting legitimate purposes of the technology. The majority of respondents noted they did not object to the Home Secretary extending the ban to further articles in the future, subject to very clear parameters for the exercise of the Home Secretary's powers such as consultation with relevant stakeholders. The then government's response to the consultation was published in November 2023[22]

[21] Preventing the use of SIM farms for fraud - GOV.UK: https://www.gov.uk/government/consultations/preventing-the-use-of-sim-farms-for-fraud

[22] https://www.gov.uk/government/consultations/preventing-the-use-of-sim-farms-for-fraud

3. SMART objectives for intervention

Proposal 1: Reform the Identification Doctrine

60. The first policy objective is to increase the ability of authorities to prosecute a corporation for criminal activity conducted by their senior management for all crimes. Extending the identification doctrine to senior management for all crimes will ensure that it appropriately covers more cases where crime is caused by the leadership through the use of corporate functions, particularly in large businesses where there are complex governance structures and decision-making is decentralised across many parts of the business. The corporate will be criminally convicted and receive a fine up to an unlimited amount to be determined by the Court. This is in addition to any sentences imposed for individuals who are also found guilty of the same offence(s).

61. Criminal convictions can exclude companies from public procurement processes and domestic and international contracts. This can have negative impacts on other parties, including investors, other employees, and even customers, heavily influencing the trajectory of a corporate beyond the fine. This will provide a clear message that corporates cannot be used to enable crime and go unpunished.

62. The second policy objective is to deter instances where corporations are used as vehicles for corrupt senior actors to conduct criminal activity. This will consist of extending the circumstances under which a corporation is prosecuted in its own right for the actions of their senior management. The greater risk of prosecution, and the corresponding penalties, will impact on senior management using the corporates as a vehicle to commit crimes. This is expected to increase deterrence and result in reduced crime.

63. The third policy objective is to provide legislative certainty. The current common law model lacks certainty beyond the general principle that the individual must be its directing mind and will at the relevant time. As the threshold for directing mind and will is hard to meet, prosecutors see risk proceeding against a large corporate with complex ownership arrangements. This has hindered the successful prosecution of corporates for crimes. The case of the Serious Fraud Office (SFO) v Barclays[23] set a very high bar for prosecutors to prove the “directing mind and will” of the company. The SFO argued that Barclays PLC and its subsidiary Barclays Bank PLC, through its Chief Executive, Chief Finance Officer and three others, had conspired to commit fraud by false representation during a capital raising exercise in the early stages of the financial crisis of 2008. The High Court rejected that these persons sufficiently met the test for directing mind and will to attribute liability. The extension of the rule to a defined class of senior management would reflect how decision-making is often dispersed across multiple controlling minds, mitigating the ability to artificially transfer, remove or create titles to escape liability.

64. Placing the identification doctrine on a statutory footing will provide legislative certainty regarding the circumstances in which the identification doctrine applies. This will not necessarily lead to an increase in new cases, as the reforms are expected to increase

[23] SFO v Barclays plc judgment (judiciary.uk): https://www.judiciary.uk/wp-content/uploads/2020/02/sfo-v-barclays-judgment-12-11-18.pdf

deterrence and subsequently reduce crime. However, it will better enable the prosecution of corporates where the law is broken.

Proposal 2: Suspension of Internet Protocol Addresses and Internet Domain Names

65. The aim of this proposal is to reduce cyber crime being facilitated through the use of domain names and IP addresses affecting individuals and businesses in the UK. Currently, there is a range of crime enabled by cyber activity, this includes computer misuse offences, phishing, fraud consumer scams, Child Sexual Abuse Materials, and dissemination of malware.

66. There is a gap in LE process and powers when looking at preventing criminal activity from domains or IP addresses as the majority of activity originates from outside the UK. At present there is no formal process for UK LE to effectively work with international partners to suspend criminal domains or IP addresses. Currently, LE and investigatory agencies are unable to formally request assistance from entities outside the UK or LE agencies in foreign jurisdictions, and many organisations internationally require court orders before they will suspend domain names or IP addresses. This means LE are unable to effectively operate internationally to suspend domains and IP addresses which are engaging in criminal activity. This frequently means that criminal activity affects UK citizens and business without UK LE being able to appropriately mitigate it. The Home Office has not been able to source appropriate data from foreign jurisdictions to allow successful international comparisons. Where other countries have different legal systems and approaches to addressing cyber crime this limits the effectiveness of comparison.

67. Domestically, private industry generally works collaboratively with LE to ensure crime is not being hosted on its platform, as this is generally against an organisation's terms of service. Whilst this collaborative process will continue, it would be helpful for investigatory agencies to be able to apply for a court order in the minority of cases where voluntary arrangements are not successful.

68. The proposed policy solution will protect those at risk of being a victim of a computer misuse offences, phishing, fraud consumer scams, Child Sexual Abuse Materials, or dissemination of malware. In the year ending June 2024, there were an estimated 952,000 incidents of computer misuse experienced by individuals in England and Wales[24].

69. This represents a statistically significant increase of 37 per cent when compared to the year ending March 2023 (745,000 offences). Unlike many other types of crime, fraud and computer misuse, by their nature, are often committed anonymously, with the offender often not having a specific target in mind. As such, there tends to be considerably less variation in victimisation rates across different demographic groups than with other crime types.

70. There is also an economic rationale for government intervention as market failure exists where domain names and IP addresses are used to enable crime such as fraud, scamming or malware distribution. These IP addresses and domain names generate

[24] Crime in England and Wales: Appendix tables - Office for National Statistics (ons.gov.uk) - https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/crimeinenglandandwalesappendixtables

significant negative externalities in the form of serious crime. Government intervention is necessary, as the issue of suspending international domain names and IP addresses cannot be resolved without intervention, and to reduce harms resulting from offences enabled by criminal domains.

Proposal 3: Ban the supply or possession of devices known as 'SIM farms' in the UK

71. The aim of the proposal is to reduce the volume and scale of fraudulent messages reaching consumers via telecommunications means (that is, calls and texts) by making it more difficult for criminals to access and use SIM farms; and giving LE powers to investigate and disrupt criminals who use SIM farms.

72. Currently, a SIM farm can be purchased online from online retailers and marketplaces, one platform was found to sell 16 slot SIM farms for £1,135.20[25]. These are usually manufactured overseas and imported through legitimate retail channels. This legislation should make it extremely difficult to purchase these devices in the UK through legitimate retailers.

73. Firstly, introducing a ban on the supply and possession of a SIM farm for non-legitimate reasons would prevent fraudsters from selling or purchasing them, blocking their access to SIM farm-enabled SMS fraud. Secondly, LE would be granted powers to seize these devices for those who already possess them, who they suspect are using them for fraud. This would raise the barrier to entry for telecoms fraud and give LE more powers to remove this technology from scammers.

74. These proposals are likely to reduce the number of mass scam texts and calls sent to consumers, reducing the total number and value of telecoms fraud by blocking the ability of scammers to access the tech to begin with. Also, by putting scammers at risk of fines, this policy will reduce the profitability of using SIM farms for fraud. Home Office expects this to reduce the total number of resulting frauds and the subsequent financial and emotional costs to victims.

75. The strategic objective of the proposed new criminal offences is to restrict the ability of criminals to access SIM farms that enable criminals to use calls and texts to target the UK public at scale. The new offences will make it more difficult for criminals to access SIM farms on online marketplaces and will provide LE with additional tools to pursue and disrupt fraudsters. It will protect the public from fraud and will enable LE agencies to respond to changing technology used by criminals, through the provision of new powers which address emerging crime types and threats.

76. It is possible to measure the number of scam SMSs blocked. This data is provided to the Home Office from operators. However, it is difficult to ascertain whether the number

[25] 4G LTE Bulk SMS Modem with 16 SIM Cards Quectel EC25 Module USB Interface Bulk SMS at Command - DirectNine - United Kingdom: https://directnine.uk/products/4g-lte-bulk-sms-modem-with-16-sim-cards-quectel-ec25-module-usb-interface-bulk-sms-at-command?gad_source=1&gclid=EAIaIQobChMI_rChndWciAMVQ4lQBh2L6hypEAQYASABEgIfdfD_BwE – accessed 12 Dec 2024

SMS Modem 32 - ChinaSkyline (sksmsgateway.com): https://sksmsgateway.com/product/sms-modem-32/ – accessed 30 Aug 2024

of scam SMSs blocked will lead to an overall reduction in the number of frauds. This is because it is difficult to ascertain the underlying flow of scams.

77. Attributing the SMS calls and messages blocked to SIM farm bans alone is difficult, as other policies aimed at reducing fraudulent SMSs and calls will be in place simultaneously. This includes fraudulent SMS filtering solutions employed by MNOs, UK Intelligence Community takedown and LE disruptions.

78. The new measure will enable the police to record SIM farms seized, enabling a measurement of the effectiveness of the new policy. Additionally, it will be possible to measure the number of prosecutions for possessions and supply of SIM farms.

79. Given the difficulty there is in defining the exact source of a scam, or where the scammers are working from and through what medium, it is not possible to define a specific timeline over which the Home Office can measure a reduction in fraud.

Diagram 1: Theory of Change – Identification Doctrine Reform

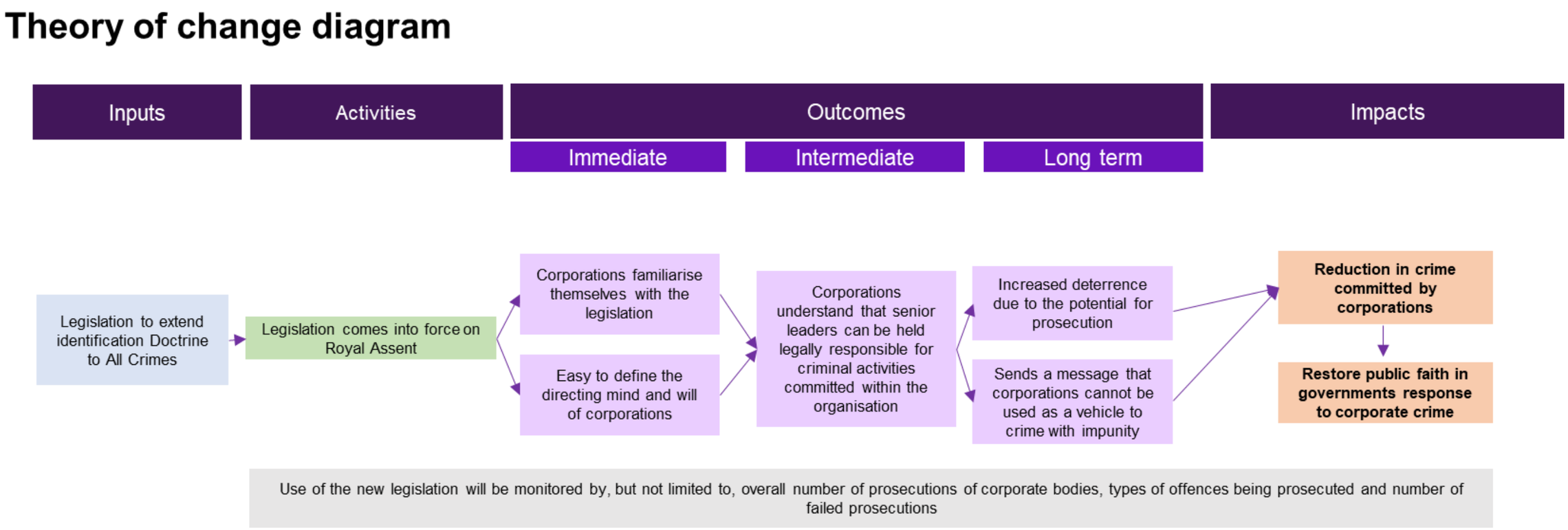
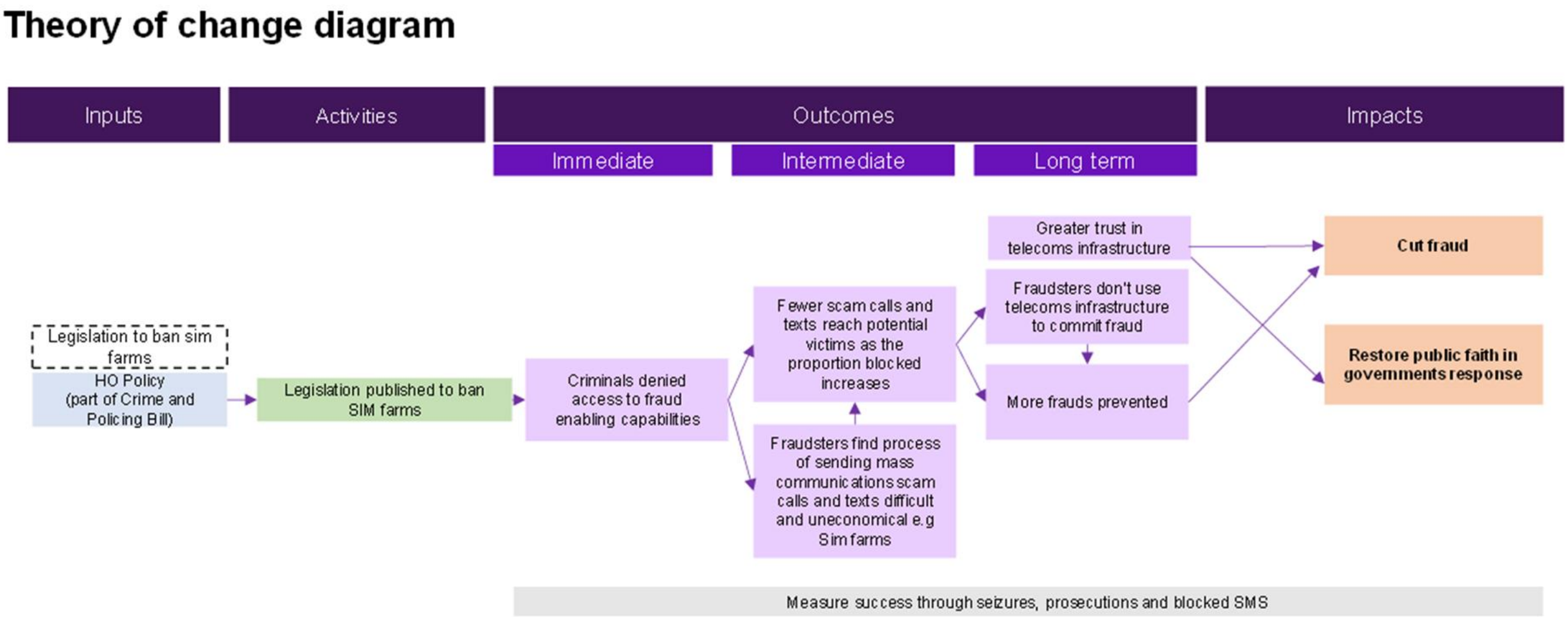


Diagram 2: Theory of Change – Ban the supply or possession of devices known as 'SIM farms' in the UK



4. Description of proposed intervention options and explanation of the logical change process whereby this achieves SMART objectives

Proposal 1: Reform the Identification Doctrine

80. The proposed option is to introduce further reforms to the identification doctrine. At present, the identification doctrine for non-economic crimes still lacks certainty. The common law is difficult to apply to the makeup of modern-day companies, particularly those that have a decentralised corporate knowledge and decision making across multiple arms of the company with different functions.

81. This reform will apply the same change in legislation introduced in the ECCT Act 2023 to all non-economic crime offences, holding a corporation liable for a criminal offence if it is committed by a senior manager. This will ensure that corporates are better held to account for all crimes and better reflects the development of the common law model that made no distinction that the identification doctrine was an economic crime regime.

82. This will create a statutory model for the identification doctrine for all criminal offences to provide legislative certainty and overcome the narrowness of the current case law by ensuring senior management are in scope of the power. The organisations in scope are corporations, and partnerships. Corporate bodies are separate entities under the law to the natural persons that are associated with it (employees or similar), enabling a chain of attribution from one to another. Partnerships can also be liable for criminal acts as entities in their own right.

83. The new model enables the prosecution of corporations for criminal offences where previous prosecutions have been unavailable. Introducing a standard test based on the Corporate Manslaughter and Corporate Homicide Act 2007[26] definition, which looks at the relative authority of the person within the organisation, reduces the ability for organisations to transfer or rename specific directing titles to avoid liability. By looking at their decision-making power rather than title, it better ensures complex governance and management structures are in scope of prosecution. This will ensure organisations cannot avoid liability for criminal offences through the use of opaque governance structures.

84. If a corporation is successfully prosecuted under the offence, it will receive a criminal conviction and fine, in addition to any sentences imposed on individuals involved in the offending. The criminal conviction can impact on other parties, including investors, other employees, and even customers.

85. Any decision to pursue a case must be made in accordance with the Code for Crown Prosecutors (or Scottish and Northern Ireland equivalents): is there enough evidence against the defendant? And is it in the public interest to prosecute?[27] The Crown

[26] Corporate Manslaughter and Corporate Homicide Act 2007: https://www.legislation.gov.uk/ukpga/2007/19/section/1

[27] The Code for Crown Prosecutors 2018: https://www.cps.gov.uk/publication/code-crown-prosecutors

Prosecution Service (CPS) has published legal guidance on how this extends to corporate prosecutions through the identification doctrine.[28]

86. It is intended that these provisions will create a new route to liability additional to the relevant common law principles and provisions upon which the present identification doctrine is founded.

87. The consultation and the Corporate Criminal Liability options paper (outlined further below in section 5) drawn up by Law Commission was based on the identification doctrine reform being extended for all crimes.[29] This is why additional consultation has not been undertaken for this Bill. The scope of the ECCT Act 2023 was limited to economic crimes only. Full reform of the identification doctrine to ensure it applies to all crimes was always the intention of government, which is why the government is now legislating for this change in the Crime and Policing Bill.

Proposal 2: Suspension of Internet Protocol Addresses and Internet Domain Names

88. The measure will allow appropriate officers to make an application to the courts for an IP address and/ or domain name to be suspended. The suspension would be for a period of up to 12 months, but this can be extended by making an application to a judge. As noted above, LE and other investigative agencies address the issue of criminals using domain names and IP addresses through voluntary partnerships.

89. The new power would strengthen existing processes by ensuring there is a formal process so that IP addresses and domain names can be suspended in international jurisdictions and where domestic voluntary arrangements are not successful.

90. Although the overall aim of the intervention is to reduce serious crime it is not possible to link the outcome of a domain name and IP address suspension to impact in terms of reduced criminality due to the wide selection of impact factors. However, evidence from the National Cyber Security Centre (NCSC) suggests that domain suspensions have a positive impact on overall internet safety[30].

91. The policy can be measured by the number of successful orders that are provided and executed per year, and in the reduction of domains and IP addresses that LE are not able to suspend. Home Office analysis, based on the number of rejected voluntary requests, suggests that LE will seek 450 orders (which could contain requests for multiple IP and domain to be suspend) to suspend IPs and domains each year. More than one IP address or domain name can be suspended on each order so the actual number of IP addresses and domain names that are suspended will be greater.

Proposal 3: Ban the supply or possession of devices known as 'SIM farms' in the UK

92. This measure criminalises the supply and possession of SIM farms in the UK, subject to a defence where there is a good reason or where adequate due diligence has been undertaken. The legislation will also allow the Secretary of State to extend the ban to other articles, where certain conditions apply. The Home Office held a public

[28] Corporate Prosecutions | The Crown Prosecution Service: https://www.cps.gov.uk/legal-guidance/corporate-prosecutions

[29] Corporate Criminal Liability - Law Commission: https://lawcom.gov.uk/project/corporate-criminal-liability/

[30] NCSC Annual Review 2022 - Resilience infographic: https://www.ncsc.gov.uk/files/NCSC_Annual%20Review%202022_Resilience_infographic.pdf

consultation on proposals to ban SIM farms and engaged extensively with a variety of stakeholders, including legitimate businesses. This option is based on the responses to the public consultation and stakeholder engagement. Their views were considered during the drafting of the offence and have developed exemptions to ensure legitimate business is not disrupted.

93. Examples of good reason to possess a SIM farm include:

- multi-SIM devices, also known as SIM gateways, used in in video production for delivering live news, events, sports, weather and traffic reports and other location-based news stories, Facebook Live and YouTube Live streaming.
- SIM gateways used only to transmit and receive voice communications over Internet Protocol (IP) networks and are not capable of sending texts or making calls or sending texts over radio frequencies. These are also known as Voice over Internet Protocol gateways and include services such as Skype, Google Talk and Microsoft Teams.
- Use of SIM farms to facilitate video transmission from security cameras; by transport providers to offer Wi-Fi on trains, trams, buses, coaches or ferries as the users will be moving between different MNOs according to which network has best reception.
- by transport and logistics businesses to track and monitor the location of freight in remote locations where it is difficult to obtain a wired internet connection – including in junction boxes beside railway lines;
- in freight yards, and at airports, and either in fixed installations or attached to mobile vehicles (such as those used to move shipping containers); and
- by communications providers who operate under OFCOM's General Conditions regime[31], to assess and maintain network security and network resilience.

94. It is likely there are further legitimate use cases that were not captured as a result of the consultation and a degree of discretion will be available to investigating authorities to determine whether a use case is exempted.

95. Suppliers to exempted sectors will be required to conduct 'reasonable checks' to ensure customers are legally entitled to use these devices.

96. Reasonable customer checks include:

a) ID verification via checks set out in UK government guidance;

b) collect physical evidence of the claimed identity (such as an identity document, like a passport) or digital evidence of the claimed identity (such as information from a personal data store);

c) checking information provided against an authoritative source or other credible verification of legitimate use case.

97. The above are examples of what is considered as "reasonable checks", but the list is not exhaustive.

[31] https://www.ofcom.org.uk/advice-for-businesses/knowing-your-rights/gen-conditions

98. Suppliers will also need to make a record of the transaction and the customer due diligence made.

99. This option will make it more difficult for criminals to access SIM farms and provide LE with additional capabilities to pursue and disrupt fraudsters. Imposing controls on the supply and possession of SIM farms will render the process of sending mass scam messages (texts and calls) more difficult and uneconomical for criminals.

100. Limiting their access to fraud enabling capabilities will limit their ability to send scam messages in bulk which will subsequently reduce the number of scam calls and texts reaching potential victims. In the longer term, this option will deter criminals from using telecoms infrastructure to commit fraud. Along with preventing fraud, this is expected to improve public trust in telecoms networks, cut fraud and improve faith in the government's response to this crime.

101. The Home Office has not been able to identify similar legislation in other countries although most countries have measures in place to counter the use of SIM farms for what is known as "international bypass fraud". Criminals use SIM farms to route international calls to the targeted network, making them appear as local calls originating within the country. This way they avoid international prices, paying instead the minimal cost of local calls. The practice is known as "international bypass fraud" and is considered an unauthorised use of the telecommunications infrastructure.

102. This is fraud against the telecoms operators, rather than consumers – thus the scope and objective are different to the department's preferred option. For example, Jordan's Telecommunications Regulatory Commission (TRC) employed a SIM box mitigation program to successfully locate and arrest SIM farm operations[32].

103. Similarly, the Communications Authority of Kenya (CA) is mandated to license all communications systems and services in the country. This includes the construction, installation and operation of international electronic communications gateway systems and services[33]. In executing this and its other responsibilities, CA is guided by the provisions of the relevant statutes, including the Kenya Information and Communications Act 1998 and the Kenya Communications Regulations 2001[34]. The limitations of a licensing regime in the UK are discussed elsewhere in this IA.

104. In Ghana, the operation of SIM boxes to bypass international call tariffs is illegal under the Electronic Communications Amendment Act 2016 (Act 910)[35]. This legislation criminalises activities that manipulate call termination to evade proper charges, such as the use of SIM farms. The National Communications Authority actively works to identify and shut down illegal SIM box operations[36]. For example, in December 2020, a joint operation led to the confiscation of SIM box equipment[37].

---

[32] 08/18/2014 18:08:47 (bswan.org), Simbox Detection Saves $1 million in Jordan | Commsrisk: https://commsrisk.com/simbox-detection-saves-1mn-in-jordan/

[33] International Gateway Systems and Services Licence - https://www.ca.go.ke/sites/default/files/CA/Licenses%20Templatses/International%20Gateway%20Systems%20and%20Services%20Licence.pdf

[34] https://www.ca.go.ke/licensing-procedures

[35] Electronic Communications (Amendment) Act, 2016, Accessed 27/02/2025: https://ghalii.org/akn/gh/act/2016/910/eng@2016-03-23

[36] https://www.cyberyoha.org/2023/04/what-is-sim-boxing.html Accessed 27/02/2025

[37] https://nca.org.gh/2020/12/04/simbox-and-international-voice-call-refilling-fraudsters-busted-in-collaborative-efforts/ Accessed 27/02/2025

105. In Australia the legality of SIM boxes relates to their intended use. While possessing or operating a SIM box is not explicitly illegal, using the device for fraud such as sending mass scam texts is unlawful. In July 2024, Australian authorities conducted a nationwide operation targeting cybercriminals who employed SIM boxes to disseminate large-scale SMS phishing attacks. This operation led to multiple arrests and the seizure of numerous SIM boxes[38]. The Australian approach is similar to section 6 of the UK's Fraud Act 2006 which makes it illegal to use an article for fraud, however, it does not pose restrictions to the possession and supply for such articles[39].

106. Other countries have adopted fraud prevention measures that could impact the misuse of SIM farms. A notable one is SIM card registration policies[40] which aim to make more difficult for criminals to acquire large numbers of SIM cards anonymously, a common tactic amongst criminal who operate SIM farms. For example, France[41] mandates that all SIM card users register their personal details with service providers to prevent anonymous communications that could facilitate criminal activities. Germany and Spain[42] enforce strict SIM card registration laws, requiring customers to present valid identification at the point of purchase. Thailand[43] and Kenya[44] mandate biometric authentication for SIM card registration to prevent fraud. Some have raised concerns that such measures may be costly, potentially intrusive, and may not always achieve their intended outcomes. In the UK, there is a possibility that SIM registration requirements could unintentionally create barriers for individuals who lack formal identification, a fixed address, or the means to visit a provider's location in person. Additionally, there are worries that the scheme might inadvertently encourage attempts to circumvent the system, such as through the use of false documents, which could pose challenges around identity verification.

107. In Singapore, all organisations sending SMS using alphanumeric Sender IDs are required to register with the Singapore SMS Sender ID Registry (SSIR)[45]. There is a one-time setup fee of S$500 for each registered organisation, and an annual charge of S$200 for each registered Sender ID[46]. If a similar scheme were to be applied in the UK, it might present some challenges for smaller businesses—such as restaurants, hair and beauty salons—that often use SMS to manage customer appointments. The scheme does not include fraudulent calls.

---

38 Nationwide policing operation targets widespread SIM box fraud | Australian Federal Police – Accesses 27/02/2025 https://www.afp.gov.au/news-centre/media-release/nationwide-policing-operation-targets-widespread-sim-box-fraud#:~:text=Policing%20agencies%20across%20Australia%20have%20joined%20forces%20in,using%20SIM%20boxes%20to%20scam%20hundreds%20of%20Australians

39 https://www.legislation.gov.uk/ukpga/2006/35/section/6

40 https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-for-development/wp-content/uploads/2021/04/Digital-Identity-Access-to-Mobile-Services-and-Proof-of-Identity-2021_SPREADs.pdf

41 Timeline of SIM Card Registration Laws | Privacy International - https://www.privacyinternational.org/long-read/3018/timeline-sim-card-registration-laws

42 Timeline of SIM Card Registration Laws | Privacy International - https://www.privacyinternational.org/long-read/3018/timeline-sim-card-registration-laws

43 https://mobileidworld.com/thailand-and-india-to-mandate-biometric-authentication-for-sim-cards-in-2025/

44 The Kenya Information and Communications (Registration of SIM-Cards) Regulations - Kenya Law - https://new.kenyalaw.org/akn/ke/act/ln/2015/163/eng@2022-12-31

45 SMS Sender ID Registry - https://www.sgnic.sg/faq/sms-sender-id-registry

46 SSIR User Agreement, Annex: Fee and Fee Payment Schedule - https://sgnic.sg/smsregistry/user-agreement .

5. Summary of long-list and alternatives

108. To avoid duplication, section 5 only includes options that were in the long-list but did not move forward to the short-list.

Proposal 1: Reform the Identification Doctrine

109. There are already significant regulatory and governance requirements on companies to detect and deter economic crime (The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, The Senior Managers and Certification Regime (SM&CR))[47]. There is also already a well-established civil recovery regime that would apply to the assets of corporations should they commit crime.[48.] Any requirement to introduce regulations or governance for every crime type would be too burdensome and costly to business, so this is not a formal option in this Bill.

110. Existing regulations also only apply to corporations in the regulated sector and a wider regime is required to apply to all corporations. In recent years, the problems with criminal corporate liability laws have been subject to extensive debate. The then government committed to looking at the rules on establishing corporate liability in the UK Anti-Corruption Plan in 2015[49].

111. In January to March 2017, the Ministry of Justice ran a call for evidence on reforming corporate liability for economic crime[50]. This consultation had no clear outcome so in November 2020, the government asked the Law Commission to examine the issue of corporate liability. The Law Commission presented ten options for reform across many different areas of law[51].

112. The Law Commission recommended introducing an offence for failure to prevent fraud and also reform of the identification doctrine. Both of these recommendations have been implemented through the ECCT Act 2023, although the latter for economic crimes only. Failure to prevent offences require businesses to enhance their corporate governance and frameworks around preventing crime, but only apply to a specific criminality (fraud, tax evasion, bribery).

113. The Law Commission's ten options are outlined below:

    0) **Retain the current general rule of criminal liability applied to corporations, the identification doctrine, as it stands (that is, 'Do nothing', Option 0):**

    Under this option, the identification doctrine as it existed would be retained without reform. The government shortlisted this option as in the absence of reform to the

---

47 The Senior Managers and Certification Regime (SM&CR) is a regulatory framework designed to enhance the accountability and conduct of individuals working in the financial services industry. This was introduced in 2016 by the Financial Conduct Authority (FCA) and the Prudential Regulation Authority (PRA).

48 Proceeds of Crime Act 2002: https://www.legislation.gov.uk/ukpga/2002/29/part/5

49 UK anti-corruption plan - GOV.UK: https://www.gov.uk/government/publications/uk-anti-corruption-plan

50 Corporate liability for economic crime: call for evidence - Ministry of Justice - Citizen Space: https://consult.justice.gov.uk/digital-communications/corporate-liability-for-economic-crime/

54 Law Commission: Corporate Criminal Liability: An Options Paper: https://lawcom.gov.uk/project/corporate-criminal-liability/

doctrine itself, the case for additional measures to deal with offences such as "failure to prevent" offences, would be more compelling.

1) **Full reform of the identification doctrine (Option 1a)**

   This is the government's preferred option and consists of extending the identification doctrine reform to all offences. Holding a corporation liable for a criminal offence if it is committed by a senior manager, will ensure that corporates are better held to account for all crimes and better reflects the development of the common law model that made no distinction that the identification doctrine was an economic crime regime.

2) **An offence of failure to prevent fraud by an associated person (Option 2)**

   An offence of failure to prevent fraud by an associated person. This offence would be committed where an associated person (who might be an employee or agent) commits an offence of fraud with intent to benefit the corporation, or to benefit a person (which might include another corporation) to whom the employee or agent provides services on behalf of the corporation. This has been taken forward and was made an offence in the ECCT Act 2023.

3) **An offence of a failure to prevent human rights abuse:**

   Under this offence, a relevant commercial organisation would be guilty of a specified offence if an associated person committed this anywhere in the world (if committed in England and Wales). The government has noted that the option was raised in the Law Commission's paper, but this option is not currently under active consideration. The extraterritorial operation of these powers would need to be properly examined before introduction can be considered and the introduction of this offence is outside the scope of this legislation.

4) **Failure to prevent ill-treatment or neglect (Department of Health and Social Care, Department for Education):**

   The government is confident that sufficient legislation already exists to prosecute ill-treatment or neglect. Under the Health and Social Care Act 2008 and within Care Quality Commission guidance, care providers must put measures in place to prevent ill-treatment and neglect in care settings. Additionally, local authorities have a legal duty to investigate instances where a vulnerable adult is at risk of abuse and offences exist to prosecute care providers who provide ill-treatment or neglect.

5) **Failure to prevent computer misuse offence:**

   The Home Office ran a call for evidence on the Computer Misuse Act 1990 (CMA 1990) in 2021 and is currently considering whether there is harmful activity that is not currently covered by the Act.[52] The government is undertaking its own detailed review of the CMA 1990, including whether statutory defences to CMA 1990 offences should be introduced.

6) **Making publicity orders available in all corporate cases:**

[52] Computer Misuse Act 1990: call for information - GOV.UK: https://www.gov.uk/government/consultations/computer-misuse-act-1990-call-for-information

Publicity orders are a requirement to publish the details of an offence. As an ancillary order, publicity orders can already be added by the Court onto a sentence depending on the circumstances of the case, including to corporate prosecutions. Although introduced under the Corporate Manslaughter and Corporate Homicide Act 2007, they have rarely been used in their own right.

The government does not see a need to make these mandatory for all corporate criminal prosecutions. Where there are successful corporate convictions for criminal and economic crime offences, agencies have historically published the outcome of cases on their public websites. These cases also receive a lot of public and press attention.

7) **A regime of administrative monetary penalties against companies:**

The government has reviewed the Law Commission's suggestion to introduce a regime of monetary penalties against companies. The proposal would see monetary penalties be administered by the SFO and the CPS. The introduction of a quasi-judicial regime superintended by prosecutors would contravene the constitutional makeup of these agencies and would not be possible without a complete transformation of their systems and purpose.

Moreover, these agencies, which have specific remits, have reported that it would be difficult to envisage circumstances where administering a monetary penalty would be appropriate. This function is executed by Regulators which have powers to impose financial penalties on corporations.

8) **Civil actions in the High Court, based on Serious Crime Prevention Orders, but involving a power to impose monetary penalties as well as preventative measures that the company would be required to take:**

An application for Serious Crime Prevention Orders can be made to the Crown Court if someone has been convicted of a serious offence and the High Court if there is an involvement in serious crime. Applications to the High Court are much less common. If prosecutors have evidence of involvement in serious crime, it may be more appropriate to pursue a conviction and attach a Serious Crime Prevention Order at a lower court.

Additionally, applications for Serious Crime Prevention Orders to introduce preventative measures are made by the SFO and CPS. Imposing monetary penalties is a power reserved by Regulators and would require a transformation of prosecutor makeup and functions to have a regulatory function.

9) **Introduce a reporting requirement requiring large corporations to report on anti-fraud procedures.**

The government continues to consider a range of proposals which encourage companies to do more to protect their customers from fraud. Reporting requirements may support this, though the government recognises the possible limitations of the approach which were acknowledged by the Law Commission to ensure that the cost to business is proportionate. This would also replicate provisions introduced by the failure to prevent fraud offence that comes into force in September 2025.

114. Having considered the Law Commission review of options, **the government decided that full reform of the identification doctrine was the preferred way forward (Option 1a)**. Option 2, a new failure to prevent fraud offence was also introduced in the ECCT Act 2023.

115. The department then considered different variations of Option 1a. These variations are set out below (Options 1b to 1c):

Option 1b:

116. The first long list option the government considered is making the corporation only liable where the intention of the senior manager was to make a gain or cause loss or expose another to loss. It might be possible to make it a condition that a company was only liable where the intention of the senior manager was to make a gain or cause loss or expose another to loss.

117. The failure to prevent bribery offence contains a requirement that the employee or agent etc pays the bribe intending "to obtain or retain business for C" or "to obtain or retain a business advantage for C". Where an offence is committed to obtain a business advantage, the offence is sufficiently closely related to economic matters that it amounted to an economic crime. However, business advantage may not be sufficient on its own.

118. There may be some instances where the employee committed offences for financial gain which couldn't really be said to be engaged in "business" – for instance, in the example of an NHS Trust executive misreporting data to get higher income for the Trust – it would be questionable whether this could be said to be "business," so Option 1b was not carried forward to short-list.

Option 1c:

119. There could be an option to combine the two tests so that the company could be prosecuted where a senior manager, in actual or apparent scope of his or her authority, engaged in the offence with intent to:

    (a) Make a gain for the organisation or another (where gain is defined in relation to the above);

    (b) Cause a loss to another;

    (c) Expose another to a risk of loss; or

    (d) Otherwise obtain a business advantage for the organisation.

120. As above, the government does not favour this option as it creates an additional stage for prosecutors as it must be proven that gain or loss must be caused to another, complicating the model in comparison to the common law. Option 1c was not taken forward.

Option 1d:

121. This option is the same as the preferred option, but with SMBs excluded. This option assesses the effectiveness of this measure while excluding any impact on the SMBs This option was deemed ineffective, as existing legislation already applies this measure, in respect of economic crime offences, to SMBs. Excluding SMBs from this measure will not materially improve their economic wellbeing as the common law identification doctrine would continue to apply. This is because this measure aims to apply the

identification doctrine more effectively to large firms, which under the common law could escape liability for criminal conduct perpetrated by senior managers due to their complex organisational structures.

Option 1e:

122. The government considered tying the criminal offence to the corporation's property. There are a limited number of instances where a senior manager would be acting in the "actual or apparent scope of their authority", that passes the evidential standard for prosecution, where they would not be using at least some physical property or identifiable element of the corporation. By including a tangible element of the corporate, it better ties the actions of the senior manager to the corporate identity, ensuring that offences are definitely out of scope where the senior manager acts on a whim. Using the corporation's property to commit the offence would require some form of economic / financial element for example, they use a service paid for by the corporate, property paid for by the corporate. The corporation itself would be benefitting or losing based on the actions of the employee, which would manifest in a form of commercial gain or loss. However, the government does not favour this option as it would create an additional stage for prosecutors as it must be proven that company property was used to commit the act, not that only committing the act was sufficient, complicating the model in comparison to the common law. This option was not taken forward as the preferred option.

Proposal 2: Suspension of Internet Protocol Addresses and Internet Domain Names

123. To avoid duplication, this section only includes options that were in the long-list but did not move forward to the short-list.

124. The government has shortlisted two options which are available to it: either 'Do nothing' and maintain the current voluntary arrangements (**Option 0)** or legislate to bring in the new power (**Option 4**).

Option 1: International only order:

125. This option would create a court order that LE agencies could apply for and use to action requests in foreign jurisdictions only. It would not be available in the UK. The benefits of this would be to protect the domestic voluntary regime whilst allowing action internationally. However, this option would not allow LE agencies to apply to the courts for an order to take down domains where the current domestic voluntary arrangements will not work. This could leave UK citizens vulnerable to crime that is facilitated through IP and domain names and would not allow agencies to cooperate across international investigations to execute joint action with partners when UK domains need to be suspended in unison. The Home Office do not believe that this option would adequately address the problem and are not recommending taking this forward.

126. Since this option has no provision for domestic orders, which limits cooperation with international partners, this option underperforms on benefits compared to the preferred option based on the SMART criteria, for example the number of successfully executed orders. While it removes the cost to UK businesses, this cost reduction is small (central £4,500) as compared to the likely benefits from joint international investigations and from additional UK suspension in the preferred option. The department's breakeven analysis shows just three fraud crimes or thirteen cyber crimes over 10 years would need to be prevented by domestic orders to breakeven for the cost to business only.

127. The Home Office has not been able to source appropriate data from foreign jurisdictions to allow successful international comparisons. Where other countries have different legal systems and approaches to addressing cyber crime this limits the effectiveness of comparison.

Option 2: Do minimum option:

128. The Home Office has considered pursuing options to limit the impact of introducing court orders, such as a Code of Practice but have concluded it would not provide sufficient assurances that the private sector would not request an order in all cases, and would potentially jeopardise the voluntary regime for takedown. It is also unclear how such a code would apply internationally since many organisations internationally require court orders before they will suspend domain names or IP addresses and so this option would not be adequate in achieving the policy aim.

Option 3: Enhancing voluntary arrangement:

129. Domestically, private industry generally works collaboratively with LE to ensure crime is not being hosted on its platform, as this is usually against the organisations' terms of service. Several respondents to the consultation supported the Home Office view that voluntary agreements should be used as a first port of call and this power should only be used as a last resort.

130. However, internet infrastructure hosting companies overseas do not always recognise informal requests from UK LE agencies, and it is not practical to have consensual relationships with every international provider in the same way that LE has domestically. There are 26 Internet Corporation for Assigned Names and Numbers (ICANN) accredited registrars in the UK, but over 1,000 internationally[53].

131. Many organisations internationally require court orders before they will suspend domain names or IP addresses and so this option would not be adequate in achieving the policy aim. Savings from judicial and LE not needing to process suspensions is likely to be outweighed by the cost of enhancing voluntary relationships, while the primary effectiveness criteria of the number of suspensions achieved is also lower.

Groups affected:

132. The main groups affected will be individuals and private institutions, these will be both in the UK and abroad. There will be a minor negative impact on costs to public bodies such as the NCA, police, HMRC, FCA and Gambling Commission of using the new power. However, this will be outweighed by the positive impacts the power will have on their capabilities and the reduction in crime this could lead to.

133. Individuals who could have been a victim of a crime due to interaction with a domain or IP address will be positively impacted by no longer being able to contact that domain or IP address. Conversely, individuals who register domains or IP addresses with the intention of using it for criminality will be affected as the domain name or IP address will be suspended.

134. It is possible for the orders to be served on international internet infrastructure organisations so those private institutions could be affected.

[53] https://www.icann.org/resources/pages/domain-name-industry-2017-06-20-en

135. Public bodies will have small efficiency savings in LE, who will more easily be able to ensure a safer internet environment through a reduction in domain names or IP addresses linked to criminality.

136. The policy is not assumed to impact legitimate small or micro businesses over and above costs incurred from business as usual.

137. Individual internet users will benefit from the reduced risk of online harm.

138. The measure will include a provision for any person affected by the order to make application to a judge to vary or discharge an order.

Proposal 3: Ban the supply or possession of devices known as 'SIM farms' in the UK

Option 1: Ban the possession and supply of SIM farms, with some exemptions. Applies only to large and largest firms (micro, small and medium firms are exempted)

139. This measure is identical to the preferred option, except that it only applies to large and largest firms.

140. This option is unlikely to be effective at achieving the objective of reducing fraudulent calls and messages. This is because it creates a loophole for fraudsters to set up micro, small and medium businesses to possess and supply SIM farms, either continuing or enabling others to continue engaging in fraud.

141. Option 1 is not taken forward to the short-list as it is deemed unfeasible in achieving its objective.

Option 2: Introduce a licensing regime

142. Under this option, businesses would have to apply and potentially pay for a licence to manufacture, use or supply SIM farms. Ofcom, the UK's communications regulator, previously explored this option for GSM gateways, of which SIM farms are a subset.

143. Their attempts were unsuccessful, and no licences have ever been issued for SIM farms or other GSM gateways. Following a review of the regulatory regime, Ofcom made a number of SIM gateways exempt from licensing under existing legislation and Home Office efforts to reverse that decision faced legal challenge from private companies – which lasted almost 20 years[54].

144. In addition, responses to the public consultation held by the Home Office in May 2023 indicate that a criminal offence would be more proportionate in line with the criminal nature of the activity that SIM farms can facilitate, and that licensing would actually be more burdensome for businesses than an exemption for legitimate uses.

145. Option 2 was not taken forward due to the complications of setting up a new regime and financial burden it may place on businesses.

Option 3: Use existing legislation

146. This option would see the Home Office instructing Ofcom to use existing powers to regulate SIM farms. In particular, under Part 3 of the Wireless Telegraphy Act 2006

[54] (VIP case, [2023] UKSC 10 R (on the application of VIP Communications Ltd (In Liquidation)) (Respondent) v Secretary of State for the Home Department (Appellant) - The Supreme Court). https://supremecourt.uk/cases/uksc-2021-0019

(regulation of apparatus: restriction orders), Ofcom and the Secretary of State have powers to impose restrictions on wireless telegraphy apparatus.

147. The Home Office explored this option with Ofcom and Home Office legal advisers and concluded that this legislation cannot be applied to SIM farms. SIM farms usually cause network congestion but not interference: the Part 3 powers are to prevent or reduce the risk of undue interference with the spectrum such as if the use brings down operators' masts or disrupts traffic on their networks. Newer versions of SIM farms have ways to avoid that kind of disruption so that MNOs do not detect them or go after them.

148. Option 3 was not taken forward as it was deemed unfeasible to use existing legislation to impose restrictions on SIM farms.

Option 4: Sender ID verification

149. Under this option, the government would promote and fund industry initiatives that aim to protect consumers, legitimate businesses and organisations falling victim to text messaging scams, through systems that verify the message header of an SMS.

150. These schemes are run by private companies and organisations and legislating to government support could be seen as interference with the free-market principles. The options can either make it voluntary or legislate to make verification of sender ID mandatory. At present, these schemes are voluntary and require a fee subscription – which adds financial burdens to small and medium businesses.

151. Businesses may choose to pass these costs on to customers by raising the prices of their products or services which can negatively impact their relationship with their customers long term. Due to their voluntary nature, they have not been taken up by businesses whose brand is often misused by criminals (such as parcel collection and delivery businesses).

152. A mandatory approach would require legislation and would have cost implications for all businesses in the UK, regardless of size. It is likely mandatory registration would be challenged by civil liberty groups as being too intrusive.

153. Option 4 is not taken forward due to its ineffectiveness in achieving policy objectives if applied voluntarily, and its cost and potential legal challenge if applied mandatorily.

6. Description of shortlisted policy options carried forward

154. To avoid duplication, section 6 only includes shortlisted options barring the preferred option, which is referred to in section 4 and 7.

Proposal 1: Reform the Identification Doctrine

155. The department shortlisted three options from the long list in Section 5, Option 0, Option 1a and Option 2. The four variations of Option 1a (Options 1b to 1e) in the long list were not shortlisted, as they would not adequately address the relevant issues that full reform of the identification doctrine will achieve.

Option 0: 'Do nothing'

156. This option consists of no government intervention through legislation. In relation to the identification doctrine, this option consisted of retaining the identification doctrine without reform. The government shortlisted this option as in the absence of reform to the doctrine itself, the case for additional measures to deal with offences such as "failure to prevent" offences, would be more compelling. However, the government decided that this option would risk the UK falling behind international standards in the prosecution of corporations' criminal activity. This is because in countries such as the US, the higher respondent superior model is in operation, which is the doctrine that the employer is liable for the acts of employees performed during the course of their employment. Option 0 was not taken forward as the preferred option, as it would not meet the strategic case for reform.

Option 1a: Full reform of the Identification Doctrine

157. The preferred option consists of extending the identification doctrine reform introduced for economic crime offences in the ECCT Act 2023, to all offences. Holding a corporation liable for a criminal offence if it is committed by a senior manager, will ensure that corporates are better held to account for all crimes and better reflects the development of the common law model that made no distinction that the identification doctrine was an economic crime regime. It also ensures that the UK does not fall behind in terms of international standards as evidenced by the higher respondent superior model, which operates in the US.

158. If a corporation is successfully prosecuted under the offence, it will receive a criminal conviction and fine, in addition to any sentences imposed on individuals involved in the offending. The criminal conviction can impact on other parties, including investors, other employees, and even customers. This will send a clear message to individuals that corporates cannot be used to enable crime and go unpunished.

Option 2: An offence of failure to prevent fraud by an associated person

159. Option 2 consists of an offence committed where an associated person (who might be an employee or agent) commits an offence of fraud with intent to benefit the corporation, or to benefit a person (which might include another corporation) to whom the employee or agent provides services on behalf of the corporation. This offence was taken forward and was introduced in the ECCT Act 2023.

Proposal 2: Suspension of Internet Protocol Addresses and Internet Domain Names

160. The department has shortlisted two options from the longlist. Other policy options would not adequately address the issue in question and would not achieve the strategic aim of the intervention.

Option 0: 'Do nothing'

161. Under the 'Do nothing' option, the majority of domestic domain suspensions would be handled under the existing voluntary relationships, but international domain suspensions and a minority of domestic cases would not be covered.

162. Unactioned requests from LE to suspend criminal domain and IP addresses would remain active allowing the continuation of offences, causing harm to UK citizens and businesses. It would also lead to victims in the UK continuing to face illegal activity and

its negative consequences from hostile domains and IP addresses abroad and at home, facing financial and other unquantifiable costs.

163. The 'Do nothing' option of continuing with the same arrangements has been considered, but it would not address the policy gaps seen in relation to the unactioned international and domestic requests.

164. Non-regulatory options have been explored fully and deemed insufficient.

Option 4: Introduce a new power to suspend domain names and IP addresses – this is the government's preferred option.

165. The overall policy objective is to ensure that LE in the UK can effectively suspend domain names and IP addresses both domestically and internationally in all relevant scenarios. The implementation of a new court order is considered to be the most viable option. This option will aid both the limited number of domestic cases that need judicial support, as well as scenarios where law enforcement need to work with international partners.

166. LE will be responsible for the ongoing operation and enforcement of the new arrangements, along with the appropriate related judicial arrangements. They will also be responsible for the ongoing operational engagement with industry, including the serving and subsequent action of the court order. These LE and investigative organisations will include NCA, police, HMRC, FCA and the Gambling Commission

Proposal 3: Ban the supply or possession of devices known as 'SIM farms' in the UK

Option 0: 'Do nothing'

167. Entails no government intervention either through legislation or other initiatives such as voluntary agreements. As a result, SIM farms would not be regulated, and their status would remain unchanged. Their supply would continue unrestricted, criminals would continue to have easy access to devices that enable them to send out scam texts in bulk at low cost and police would not have additional capabilities to disrupt criminals in possession of SIM farms.

168. Option 0 was not taken forward as the preferred option, as it would not meet the objectives set out in the strategic case.

Option 5: Support industry initiatives to identify and block scam texts.

169. The government and the telecommunications industry have already introduced non-regulatory measures to address criminals abusing calls and texts to target the UK public at scale. The Telecommunications Sector Charter published in October 2021[55], was a voluntary agreement with telecommunications providers to reduce fraud. Under the Charter, the sector introduced firewalls that detect and stop scam texts from reaching customers. The Charter ended in December 2023 and the government is considering a second Charter which would include a commitment for operators to develop further measures to identify and block scam texts and calls.

170. However, the Charter actions are subject to agreement with telecoms operators and its voluntary nature does not compel operators to deliver the actions. Furthermore, the Charter only applies to signatories. While the firewalls offer protections and have led to

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

a reduction in scam texts, they are not available to all mobile network customers in the UK and they do not cover scam calls. Moreover, they do not pose any barriers to criminals in terms of procuring SIM farms.

171. Option 5 was not taken forward as the preferred option as its voluntary nature would not compel operators to deliver on the actions, nor does it have a comprehensive coverage in the UK.

7. Regulatory scorecard for preferred option

Proposal 1: Reform the Identification Doctrine

Part A: Overall and stakeholder impacts

(1) Overall impacts on total welfare		Directional rating Note: Below are examples only
Description of overall expected impact	The overall impact is dependent on the net benefits minus the costs. There are monetised costs owing to familiarisation with the policy for businesses. There are also non-monetised costs, which accrue in the form of increased public sector spending in the CJS system. However, the latter are likely to be insignificant. The benefits are all non-monetised as the Home Office has so far not been able to source well evidenced estimates for the number and type of criminal acts that this legislation will prevent. This is because the data on failed prosecutions, due to the challenges under the current common law identification doctrine, cannot easily be identified from CPS records. As highlighted in the Strategic Case, it would be costly to collect data on all potential cases the identification doctrine could apply to, as this would require consultation with users of any law in England and Wales. The benefits as a result of this legislation are likely to accrue in the form of reduced criminality as a result of greater deterrence. This greater deterrence is likely to arise from the increased potential for prosecution for corporations for criminal acts due to this legislation. The public sector is expected to incur costs as a result of the legislation enabling a greater number of corporate prosecutions, and therefore increase the burden on law enforcement and the CJS. This cost has not been quantified due to an absence of evidence for the likely scale of the increase. However, consultation with the CPS and SFO found that additional court cases are expected to be low and any additional costs are expected to be modest. In terms of potential unintended consequences and risks, there is a possibility that senior individuals of corporations may perceive an increase in risk in operating in the UK due to the identification doctrine reforms and senior decision makers of corporations may look to move their organisation outside of the UK's jurisdiction to avoid being subject to the reforms. However, the government has not been made aware of any individuals or corporations who have left the UK as a result of either the initial reform in the ECCT Act 2023, or of this proposed reform. The benefits of introducing wholesale identification doctrine reform mitigate this potential risk because it encourages	**Positive** **Based on all impacts (incl. non-monetised)**

	compliance and provides a clear message to individuals that corporates cannot be used to enable crime and go unpunished. Without reform, there is also a risk that the UK could fall behind in terms of international standards in the prosecution of organisations involved in criminal activity. For example, the United States has the respondent superior model in place, the legal doctrine that the employer may be held responsible for the actions of its employees performed within the actions of employment. If full reform of the identification doctrine is not undertaken, the UK may lack an ability to bring proceedings in high-profile cross border criminal cases in support of partner agencies such as in the United States Department of Justice. Overall, the non monetised impact is likely to be positive as the benefits from reduced corporate fraud from the deterrence is likely to outweigh the monetised costs to business and the unmonetised costs to the public sector from increased CJS costs.	
Monetised impacts	The only monetised impact is the cost of familiarisation with the new measure for businesses. This is likely to be negative, with and NPSV between -£0.2 million and -£1.2 million (Price Base 2025/26; PV Base 2025/26).	**Negative** **Based on likely £NPSV**
Non-monetised impacts	**Benefits** Currently, there is an absence of data on the incidence and resulting losses of the corporate crimes in scope of this legislation. As highlighted in the Strategic Case it would be costly to collect data on all potential cases the doctrine could apply to, as this would require consultation with users of any law in England and Wales. It has not been possible to monetise benefits or the societal costs arising from the current limitations. A greater risk of prosecution and resulting sanctions (which are not limited to monetary penalties and also include exclusion from public procurement processes and disgorgement of profits) will strengthen the deterrent and reduce corporate crimes. There is an absence of data on the incidence and resulting losses of the corporate crimes in scope of this legislation. This means that the Home Office is unable to quantify the potential types or number of corporate crimes avoided, and the resulting benefits to society, resulting from greater deterrence. To provide an indicative sense of value for money annex A.3. includes a breakeven analysis of the identification doctrine's monetised costs relative to the unit cost of fraud. Despite fraud and other economic offences being covered previously by the ECCT Act 2023 and being out of scope of this legislation. In the absence of well evidenced data on which crime types may be avoided, the unit cost of Fraud was deemed to be the best available unit cost of crime for such an analysis. In the central scenario with monetised costs of £0.5 million, the identification doctrine would have to prevent 348 fraud offences to breakeven (116 and 858 frauds in the low and high scenarios respectively). This approximate analysis is intended to	**Positive**

	demonstrate that only a relatively small number of offences must be prevented to recover the monetised costs of the policy. If the identification doctrine prevents non-economic offences in scope of a similar value then the policy could breakeven and potentially deliver considerable societal benefit. Whilst the ECCT Act 2023 is being implemented and could provide more tangible evidence of impact, the scope of this legislation is focussed on economic crimes only so cannot help to assess the impact of a reform to prevent a broader range of crimes. **Costs and Risks** Previous implementation evidence from economic crime reforms such as the Failure to Prevent Bribery offence could not be used as an evidence base to consider wider costs beyond those identified in the monetised impacts section as this legislation differs significantly. For example, this legislation is not based around requiring organisations to show that reasonable measures have been put in place to act as a defence against prosecution in the case of bribery taking place in the organisation. The public sector is expected to incur costs as a result of the legislation enabling a greater number of corporate prosecutions, and increase the burden on law enforcement and the CJS. This cost has not been quantified due to an absence of evidence for the likely scale of the increase However, consultation with the CPS and SFO found that additional court cases are expected to be low and any additional costs are expected to be modest. In terms of potential unintended consequences and risks, there is a possibility that senior individuals of corporations may perceive an increase in risk in operating in the UK due to the identification doctrine reforms and senior decision makers of corporations may look to move their organisation outside of the UK's jurisdiction to avoid being subject to the reforms. However, the government has not been made aware of any individuals or corporations who have left the UK as a result of either the initial reform in the ECCT Act 2023, or of this proposed reform.	
Any significant or adverse distributional impacts?	No, this policy is expected to be applied nationally, with no regional impacts. No groups from the protected characteristics are disproportionately impacted. No distributional effects expected.	**Neutral**

(2) Expected impacts on businesses		
Description of overall business impact	The overall impact is dependent on the benefits minus the costs. The overall business impact is likely to be positive as the benefits from reduced criminality through deterrence are likely to outweigh the cost of familiarisation with the policy.	**Positive**
Monetised impacts	Monetised impact will be negative as the policy does impose costs on businesses in the form of familiarisation with the new measure. This familiarisation cost accrues from the anticipated time it will take the appropriate staff members to familiarise with the guidance in a low, central and high scenario. Whilst only large businesses are in scope of this legislation, the number of staff obligated to read the guidance is assumed to be increasing in line with overall organisation size. Whilst more detail on this cost estimate is provided in Annex A.3., the NPV of costs is between -£0.2 million and -£1.2 million (Price Base 2025/26; PV Base 2025/26).	**Negative** **Based on likely business £NPV**
Non-monetised impacts	Non monetised impact for businesses will be positive as it comprises of reduction in criminality through improved deterrence from the new measure.	**Positive**
Any significant or adverse distributional impacts?	No, there are no sectoral business or regional business impact from the measure.	**Neutral**

(3) Expected impacts on households		
Description of overall household impact	There may be a positive impact on households as this measure may reduce losses experienced by households from fraud carried out by or within firms. The scale of the impact is uncertain. These policies are not expected to have any cumulative effect on households.	**Positive**
Monetised impacts	No significant direct impact on household expected.	**Neutral** **Based on likely household £NPV**
Non-monetised impacts	There may be a positive impact on households as this measure may reduce losses experienced by households from fraud carried out by or within firms. The scale of the impact is uncertain.	**Positive**
Any significant or adverse distributional impacts?	No significant direct impact on household expected.	**Neutral**

Part B: Impacts on wider government priorities

Category	Description of impact	Directional rating
Business environment: Does the measure impact on the ease of doing business in the UK?	Attractiveness of business environment: there is a possibility that senior individuals of corporations may perceive an increase in risk in operating in the UK due to the identification doctrine reforms. Senior decision makers of corporations may look to move their organisation outside of the UK's jurisdiction to avoid being subject to the reforms. However, the benefits of introducing wholesale identification doctrine reform mitigate this potential risk because it encourages compliance and provides a clear message to individuals that corporates cannot be used to enable crime and go unpunished. Overall, the reforms will make the UK a safer and more stable economic environment for businesses. No significant barriers to entry. No significant effect on market concentration and competition No significant impact on foreign investment. No significant impact on the scope for businesses to bring innovative products and services to market. In aggregate, this policy should make the business environment better.	**Supports**
International Considerations: Does the measure support international trade and investment?	No significant impact on international trade and investment.	**Neutral**
Natural capital and Decarbonisation: Does the measure support commitments to improve the environment and decarbonise?	No significant impact on natural capital or decarbonisation expected.	**Neutral**

Proposal 2: Suspension of Internet Protocol Addresses and Internet Domain Names

Part A: Overall and stakeholder impacts

(1) Overall impacts on total welfare		Directional rating Note: Below are examples only
Description of overall expected impact	The increase in domain name / IP address suspensions will lead to a reduction in cyber enabled fraud and remove nodes in criminal enterprises for cyber enabled fraud, breakeven analysis is undertaken in the benefits section to illustrate the possible scale of benefits. Increased confidence in UK Government and ability to police online activity.	**Positive** **Based on all impacts (incl. non-monetised)**
Monetised impacts	Total costs of the scheme are estimated to lie in a range of **£0.38 to £0.42 million** with a **central estimate of £0.40 million** above baseline (PV over 10 years). These costs are made up of ongoing agency and judicial costs of processing and signing off suspensions and year one familiarisation costs to the public sector and ongoing costs of suspending domain names and IP addresses for industry.	**Negative** **Based on likely NPSV of -£0.40m**
Non-monetised impacts	Benefits are not monetised or included in the NPSV due to difficulties in attributing impact of domain and IP address suspensions to outcomes in terms of crime avoided. Breakeven analysis is presented within the analysis section to show how many offenses would have to be avoided to pay for the policy. Benefits have not been calculated as it is not possible to link the outcome of a domain name and IP address suspension to impact in terms of reduced criminality due to a selection of factors. Lack of knowledge of when most of the harm occurs in the lifecycle of the domain and IP address, backfill of new domains and IP addresses, and variation in harm in domains and IP addresses. As such, breakeven analysis has been performed to give a scale of the number of offences that would have to be avoided for the program to cover its costs. Although the estimated increase in the number offences avoided cannot be reliably estimated, there will be an increase and consequently a monetary benefit in terms of crime avoided.	**Positive**

Any significant or adverse distributional impacts?	No	**Neutral**
(2) Expected impacts on businesses		
Description of overall business impact	The majority of domestic suspensions will be dealt with under existing voluntary relationships; however, a minority will come into scope of the measure following ministerial consideration. Based on the number of historic domestic cases in which the power would have been used or how many domestic cases have been refused due to lack of judicial backing, the NCA expect between 3 and 12 domestic domain suspensions and 1 domestic IP address suspension, HMRC and NPCC do not expect any domestic domain or IP address suspensions. These cases will impose a cost to UK businesses, domain registries and registrars which will have to suspend the IP addresses and domain names. However, the increase in domain name /IP address suspensions will lead to a reduction in cyber enabled fraud and remove nodes in criminal enterprises for cyber enabled fraud.	**Positive**
Monetised impacts	Present value costs to business over 10 years could fall between £2,000 (£0.00 million) in the low case and £7,000 (£0.01 million) in the high case with a central estimate of £5,000 (£0.00 million).	**Neutral** **Based on likely business NPV of -£5,000 (£0.0m)**
Non-monetised impacts	Many domain and IP address suspensions resulting from legislation are expected to be international so the cost to international domain hosting entities to take down domains and IP address is not captured as it falls outside of the UK. Benefits have not been calculated as it is not possible to link the outcome of a domain name and IP address suspension to impact in terms of reduced criminality due to a selection of factors. Lack of knowledge of when most of the harm occurs in the lifecycle of the domain and IP address, backfill of new domains and IP addresses, and variation in harm in domains and IP addresses. As such, breakeven analysis has been performed to give a scale of the number of offences that would have to be avoided for the program to cover its costs. Although the estimated increase in the number of offences avoided cannot be reliably estimated, there will be an increase and consequently a monetary benefit in terms of crime avoided.	**Positive**

Any significant or adverse distributional impacts?	No, the policy is not assumed to impact legitimate small or micro businesses over and above costs incurred from business as usual. There should be little or no cost burden for a registry or registrar acting upon the order. The processes can generally be automated and there is an existing process for ICANN to waive the nominal fee they charge registries upon the creation of a domain name, when the action is in support of a court order issued to LE. The Home Office does not consider that there is any requirement for the registry/registrar to be able to refuse to comply with the order on costs grounds. Similarly, the department has sought to limit the impact of the cost implications for businesses of having to purchase new IP addresses by restricting the length of time for which an order is made and ensuring the IP is retained by the Local Internet Registries for future use.	**Neutral**
(3) Expected impacts on households		
Description of overall household impact	The increase in domain name /IP address suspensions will lead to a reduction in cyber enabled fraud and remove nodes in criminal enterprises for cyber enabled fraud, breakeven analysis is undertaken in the benefits section to illustrate the possible scale of benefits to households and individuals. These policies are not expected to have any cumulative effect on households.	**Positive**
Monetised impacts	Not calculated.	**Neutral**
Non-monetised impacts	Benefits have not been calculated as it is not possible to link the outcome of a domain name and IP address suspension to impact in terms of reduced criminality due to a selection of factors. Lack of knowledge of when most of the harm occurs in the lifecycle of the domain and IP address, backfill of new domains and IP addresses, and variation in harm in domains and IP addresses. As such, breakeven analysis has been performed to give a scale of the number of offences that would have to be avoided for the program to cover its costs. Although the estimated increase in the number offences avoided cannot be reliably estimated, there will be an increase and consequently a monetary benefit in terms of crime avoided.	**Positive**
Any significant or adverse distributional impacts?	No	**Neutral**

Part B: Impacts on wider government priorities

Category	Description of impact	Directional rating
Business environment: Does the measure impact on the ease of doing business in the UK?	This policy should increase public confidence in the UK's ability to police online activity and safety abroad. This could lead to more online economic activity, increasing sales for online businesses.	**Supports**
International Considerations: Does the measure support international trade and investment?	This policy should increase public confidence in the UK's ability to police online activity and safety abroad resulting in greater willingness to trade and invest in the UK.	**Supports**
Natural capital and Decarbonisation: Does the measure support commitments to improve the environment and decarbonise?	No impact	**Neutral**

Proposal 3: Ban the supply or possession of devices known as 'SIM farms' in the UK

Part A: Overall and stakeholder impacts

(1) Overall impacts on total welfare		Directional rating Note: Below are examples only
Description of overall expected impact	The overall impact is dependent on the benefits minus the costs. The benefits of the preferred option are unmonetisable, as there is uncertainty around how many frauds will be prevented, and therefore its monetised benefits. The costs are monetisable and likely to be incurred from familiarisation with the new legislation. On balance, unmonetised benefits are likely to outweigh the monetised costs.	**Positive** **Based on all impacts (incl. non-monetised)**
Monetised impacts	Total monetised impacts are likely to be small but negative due to a monetisable cost of familiarisation and no monetisable benefits. The range for NPSV is -£0.01m to -£0.04m (Price Base 2025/26; PV Base 2025/26).	**Negative** **Based on likely £NPSV**
Non-monetised impacts	The non monetised impact is highly likely to be positive due to unmonetised benefits of reduced loss of receipt to fraud for businesses and individuals and improved wellbeing. This benefit is unmonetised as the extent to which the SIM farm ban will reduce the volumes and harm of fraud is unknown. Whilst this uncertainty exists, fraud remains the most common CSEW recorded crime. The 2023 Fraud Strategy included an estimate of the total economic and social cost of fraud to individuals in England and Wales of £6.8 billion in 2019/20 for an estimated 3,675,000 offences[56]. As this doesn't account for Fraud against businesses, the true cost of fraud is likely to be higher. A breakeven analysis can be calculated to suggest how many frauds the policy must avoid to recover its monetised cost. This calculation instead uses the Economic and Social Costs of Crime (ESCC) unit cost for Fraud of £1,290 per offence in 2015/16 prices (again this is an estimate of fraud against individuals only, not businesses)[57]. The ESCC figure is used instead of that from the more recently published fraud strategy as it is more granular, with it being possible to isolate out the constituent components. Taking the £1,290 cost per fraud offence, the *"anticipation"* component of this cost is deducted as this is incurred before the crime takes place and therefore won't be impacted by any reduction to the volume of crime. The unit cost of Fraud	**Positive**

[56] Fraud Strategy: stopping scams and protecting the public - GOV.UK: https://www.gov.uk/government/publications/fraud-strategy/fraud-strategy-stopping-scams-and-protecting-the-public

[57] The economic and social costs of crime: https://assets.publishing.service.gov.uk/media/5b684f22e5274a14f45342c9/the-economic-and-social-costs-of-crime-horr99.pdf

	excluding anticipation costs is therefore £1,070 in 2015/16 prices. Uplifting this value to 2025/26 prices using the GDP Deflator gives an average loss of £1,450.25. An approximate breakeven analysis therefore suggests that the legislation would only need to avoid 25 frauds to recover the monetised costs in the high scenario. Whilst there are additional costs that cannot be monetised, it is not anticipated that these would significantly increase the number of frauds that would have to be avoided for the policy to break even. Considering again the large scale of Fraud, any reductions in incidences attributable to this legislation could have significant societal benefits. Non-monetised cost is likely to be small from the reduction in the unwitting sale of SMS cards to fraudsters. Additionally, there may be a small cost due to an additional due-diligence criteria. Criminal Justice Costs are expected to be negligible, with the Home Office anticipating a relatively small number of cases per year, though an absence of evidence means it is not possible to provide a quantitative estimate. The offence will carry the penalty of an unlimited fine in England or the maximum possible fine in Scotland. The offence will not carry the risk of custodial punishment.	
Any significant or adverse distributional impacts?	No, this policy is expected to be applied nationally, with no regional impacts. No groups from the protected characteristics are disproportionately impacted. No distributional effects expected.	**Neutral**
(2) Expected impacts on businesses		
Description of overall business impact	The overall impact is dependent on the benefits minus the costs. There are no monetised impacts on businesses due to limited data on the effect of SIM farm on business. Net on monetised impacts, in aggregate, is positive from cost savings to firms from SIM farm bans. The overall effect on businesses is likely to reflect the non-monetised impact of the policy on business.	**Positive**
Monetised impacts	There is insufficient data that assesses the benefits of SIM farms on businesses. As a result, there are no monetised benefits on businesses. Minor familiarisation costs to the private sector are expected as distributors, suppliers and users will need to familiarise themselves with the legislation and put in place processes for 'reasonable checks' going forwards. An absence of evidence means this has not been quantified.	**Negative** **Based on likely business £NPV**
Non-monetised impacts	The consultation included a call for evidence to collect information and data on the potential impacts of the SIM farm ban. The government response to the consultation concluded that due to the limited amount of evidence received, there remains uncertainties in relation to the impact of the proposal on businesses and the costs associated with introducing and	**Positive**

	implementing the ban[58]. The impact assessment therefore presents the non-monetised impacts on businesses from the proposed option. Costs For MNOs, the effect of reduction in revenue from fewer purchases of SIM cards to facilitate fraud SMSs and calls. • Familiarisation cost for businesses in the UK of benefits • Minimal due-diligence costs to verify genuine use, as most of due diligence is already carried out by businesses. • 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. Benefits • The cost savings to MNOs (and other firms) from fewer frauds that released by the SIM farms.	
Any significant or adverse distributional impacts?	No, there are no sectoral business or regional business impact from the measure.	**Neutral**
(3) Expected impacts on households		
Description of overall household impact	Households are likely to have a positive impact due to lower incidents of and losses to fraud. There are no costs for households the policy is targeted at business. These policies are not expected to have any cumulative effect on households.	**Positive**
Monetised impacts	N/A, due to insufficient data.	**Neutral** **Based on likely household £NPV**
Non-monetised impacts	Positive impact due to a reduction in fraud received by customers and fewer losses to SIM farm related losses.	**Positive**
Any significant or adverse distributional impacts?	No, this policy is expected to be applied nationally, with no regional impacts on households. No distributional effects expected.	**Neutral**

Part B: Impacts on wider government priorities

[58] Preventing the use of SIM farms for fraud: government response: https://assets.publishing.service.gov.uk/media/655f3b45dcc6be000d5d1134/Government_Response_to_the_Consultation__Preventing_the_use_of_SIM_farms_for_fraud_.pdf

Category	Description of impact	Directional rating
Business environment: Does the measure impact on the ease of doing business in the UK?	Attractiveness of business environment: The measure may make UK potentially less attractive to businesses who rely on SIM farms. However, there are exemptions designed into the policy which mitigate against the negative effect of the policy. Additionally, the UK business environment may also be considered safer due to lower fraud in circulation. The net effect of this measure on attractiveness of business is therefore positive. Legitimate business uses are exempt, therefore, it is not expected that this legislation will alter legitimate business behaviour. Consequently, it is not expected that this legislation will have any innovation impacts. No significant barriers to entry. No significant effect on market concentration and competition. No significant impact on foreign investment. No significant impact on the scope for businesses to bring innovative products and services to market. In aggregate, this policy should make the business environment better.	**Supports**
International Considerations: Does the measure support international trade and investment?	Following consultation with Department for Business and Trade officials, the Home Office can confirm that these measures do not require World Trade Organisation notification or handling. In particular, it does not require notification/handling to the Committee on Technical Barriers to Trade (TBT).	**Neutral**
Natural capital and Decarbonisation: Does the measure support commitments to improve the environment and decarbonise?	No significant impact on natural capital or decarbonisation expected.	**Neutral**

8. Monitoring and evaluation of preferred option

Proposal 1: Reform the Identification Doctrine

211. This measure will come into force two months after Royal Assent of the Bill, and the Home Office suggest the government complete a review involving an assessment of use and a process evaluation around two years thereafter to give time for there to be sufficient use.

212. During this two-year period, key metrics will be monitored to understand use of the new legislation. Key metrics include but are not limited to:

    a. Overall number of prosecutions of corporate bodies.

    b. Types of offences being prosecuted.

    c. Number of failed prosecutions.

213. Data will be gathered by engaging with the Crown Prosecution Service and Serious Fraud Office who will be asked to supply data across the two year period. The government will also review the effectiveness of the legislation within five years of Royal Assent according to the legislative scrutiny process which will contain detail on the metrics above and qualitative data on enforcement authority experience in applying the new corporate liability provisions to their caseloads.

214. The Home Offices evaluation framework focuses on assessing whether two key aims have been achieved: whether the reforms have enabled prosecution of corporate bodies, and whether the powers have had affected corporate action and behaviour. This is likely to be addressed primarily through a process evaluation, as the number of prosecutions is anticipated to be small, and if the measure is successful at changing behaviour then there may be no increase in prosecutions.

215. Process evaluation: this is likely to include qualitative work to understand views on the measure, its usage, any remaining barriers and any unintended consequences. This would likely involve key members of the CJS, such as CPS, LE and members of the judiciary. Further qualitative work with businesses could be carried out, and would aim to understand the clarity of the powers, how this has affected the business, and any changes made as a result, including addressing a potential unintended consequence identified that this may make business more likely to move operations outside of the UK.

Proposal 2: Suspension of Internet Protocol Addresses and Internet Domain Names

216. Home Office officials are working with stakeholders to develop operational guidance on how suspension of Internet Protocol Addresses and Internet Domain Names will be implemented in practice. The power is expected to come into effect around six months after the Act receives Royal Assent to allow time for new criminal court procedure rules to be introduced. A post implementation review of the policy will take place two years after the power has been introduced.

217. This two-year period will allow time for implementation to be monitored and for a sufficient number of orders to be completed. Possible metrics to monitor over this time period could include the number of successful orders that are provided and executed and the number of domains and IP addresses that LE are unable to suspend.

218. The nature of further evaluation undertaken will be assessed based on the feasibility and proportionality of a process or impact evaluation.

219. An evaluation may include informal consultation with the main affected agents, a consideration and discussion of unintended consequences and the wider effects of the policy and a discussion of the scale of any identified problems. Although the overall aim of the intervention is to reduce serious crime it is not possible to link the outcome of a domain name and IP address suspension to impact in terms of reduced criminality due to the wide selection of impact factors. Therefore, an impact evaluation is not likely to be feasible as it would be difficult to attribute any changes in cyber crime levels to the suspension of IP addresses and internet domain names.

220. Any evaluation carried out will be proportional to the impact of the policy in line with Better Regulation Framework requirements.

Proposal 3: Ban the supply or possession of devices known as 'SIM farms' in the UK

221. Home Office officials are working with stakeholders to develop guidance which will describe how the government's ban of possessing and supplying SIM farms will be implemented in practice. The offences are expected to come into effect six months after the Act receives Royal Assent to allow time to publish associated guidance. A post implementation review of the policy will take place two years after the offence comes into effect.

222. The two-year period will allow time to monitor its implementation. Data to be monitored over this time period could include metrics such as:

    a. the number of SIM farms seized,

    b. prosecutions for possession, and

    c. supply numbers of legitimate SIM farms.

    d. The Home Office will also explore using data available via the new national police reporting service for fraud and cyber crime that will replace Action Fraud, and is due to be operational in 2025.

223. The aim of the legislation is to make it more difficult for criminals to access SIM farms, and give LE additional tools to disrupt fraudsters. Therefore the Home Office's evaluation framework focusses on evaluation of how and whether the ban has resulted in these two aims. The Home Office suggest that a proportionate evaluation would involve:

    1) A process evaluation: To understand how LE use additional tools to disrupt fraudsters. This would have the following research priorities: to understand how the guidance has been implemented, any issues, how LE have used these additional tools, and any barriers to their use. This would likely have two main components:

        a. Understanding LE perspectives and experience of using the powers, any barriers to use, and any improvements to the guidance. This could include an initial survey to gauge use across a wide range of LE, and obtain volunteers for participating in further qualitative work, either focus groups or interviews.

b. Understanding wider stakeholder views, and any difficulties in continuing with legitimate use. This might include groups such as distributors, suppliers and users of SIM farms. This would likely be carried out through focus groups.

2) Impact evaluation: Due to the difficulty in attributing impact of any changes in fraud levels to the banning of SIM farms, the Home Office suggest a well evidenced impact evaluation will likely be out of scope. However, monitoring data will be assessed to give some indication as to what changes may have occurred. Exact methods will need to be defined when the powers have bedded in, and the Home Office can assess use numbers, but a theory-based approach, rather than a quasi-experimental approach is likely to be more feasible.

9. Minimising administrative and compliance costs for preferred option

Proposal 1: Reform the Identification Doctrine

224. Minor familiarisation costs are expected, as large organisations will need to familiarise themselves with the new legislation. No ongoing costs have been identified.

225. It is expected that costs to small and medium organisations will be negligible as they can currently be effectively prosecuted under the current identification doctrine.

226. No public sector set up costs have been identified.

Proposal 2: Suspension of Internet Protocol Addresses and Internet Domain Names

227. There will be a minor negative impact on costs to public bodies using the new power, including the NCA, police, HMRC, FCA and Gambling Commission. This will be outweighed by the positive impacts the power will have on their capabilities and the reduction in crime that this could lead to. As the majority of domestic suspensions will be dealt with under existing voluntary relationships there will not be any additional burdens in complying with the regulation. Familiarisation costs to business are not expected as domain and IP address registries perform suspensions as part of their business-as-usual operations.

228. It is possible for the orders to be served on international internet infrastructure organisations so those private institutions could be affected.

229. Total costs of the scheme are estimated to lie in a range of £0.37 to £0.41 million with a central estimate of £0.39 million above baseline (PV over 10 years). These costs are made up of ongoing agency and judicial costs of processing and signing off suspensions and year one familiarisation costs to the public sector and ongoing costs of suspending domain names and IP addresses for industry.

230. Public bodies will have small efficiency savings in law enforcement, who will more easily be able to ensure a safer internet environment through a reduction in domain names or IP addresses linked to criminality.

231. The majority of domestic suspensions will be dealt with under existing voluntary relationships; however, a minority will come into scope of the measure following ministerial consideration. Based on the number of historic domestic cases in which the power would have been used or how many domestic cases have been refused due to lack of judicial backing, the NCA expect between 3 and 12 domestic domain suspensions and 1 domestic IP address suspension, HMRC and NPCC do not expect any domestic domain or IP address suspensions. These cases will impose a cost to UK businesses, domain registries and registrars which will have to suspend the IP addresses and domain names. However, the increase in domain name /IP address suspensions will lead to a reduction in cyber enabled fraud and remove nodes in criminal enterprises for cyber enabled fraud.

232. The policy is not assumed to impact legitimate small or micro businesses over and above costs incurred from business as usual.

233. There should be little or no cost burden for a registry or registrar acting upon the order. The processes can generally be automated and there is an existing process for ICANN to waive the nominal fee they charge registries upon the creation of a domain name, when the action is in support of a court order issued to LE.

234. The Home Office does not consider that there is any requirement for the registry/registrar to be able to refuse to comply with the order on costs grounds. Similarly, the Home Office has sought to limit the impact of the cost implications for businesses of having to purchase new IP addresses by restricting the length of time for which an order is made and ensuring the IP is retained by the Local Internet Registries for future use.

Proposal 3: Ban the supply or possession of devices know as 'SIM farms' in the UK

235. Minor familiarisation costs to the private sector are expected as distributors, suppliers and users will need to familiarise themselves with the legislation and put in place processes for 'reasonable checks' going forwards. An absence of evidence means this has not been quantified.

236. One-off familiarisation costs are expected as the change in legislation will mean that Border Force staff, conducting routine searches and checks at the border, will have to familiarise themselves with how the legislation will be implemented.

237. CJS costs are expected to be negligible. As the Home Office anticipate that there will be a relatively small number of cases per year for use and possession of SIM farms. Although the absence of evidence means it is not possible to provide a quantitative estimate.

238. The College of Policing ensure that all new legislation is incorporated into the national policing curriculum as a matter of course and falls within existing budgets. The additional public cost of training for this policy is expected to be negligible.

239. It is important to note that there is no evidence that the fraudsters using these devices are obtaining them from the legitimate UK suppliers, which will be exempted under the proposals. The Home Office has conducted an extensive engagement process with legitimate distributors, suppliers and users of these devices. The majority of them already have due diligence measures in place to record and monitor business transactions.

240. The Home Office is working closely with these businesses to develop guidance to assist the enforcement of the offence. The Home Office will delay commencement for six months after Royal Assent to enable businesses to comply with the legislation. Familiarisation costs for legitimates businesses are expected to be negligible.

Declaration

Department: Home Office

Contact details for enquiries:

CrimeandPolicingBillTeam@homeoffice.gov.uk

Minister responsible:

Dan Jarvis MP, Minister for Security

I have read the Impact Assessment and I am satisfied that, given the available evidence, it represents a reasonable view of the likely costs, benefits and impact of the leading options.

Signed: 

Date: 30 October 2025

Summary: Analysis and evidence

Proposal 1: Reform the Identification Doctrine

Price base year: 2025/26

PV base year: 2025/26

This table may be reformatted provided the side-by-side comparison of options is retained		**0. Business as usual (baseline)**	**4. Preferred way forward (if not do-minimum)**
Costs (£m)	Low	0	0.2
	High	0	1.2
	Best	0	0.5
(Distinguish between setup and ongoing costs, as well as private/public costs)			All estimated costs are familiarisation costs that fall on the private sector.
Benefits (£m)	Low	0	0
	High	0	0
	Best	0	0
(Distinguish between setup and ongoing benefits, as well as private/public benefits			
Net present social value (£m)	Low	N/A	-0.2
	High	N/A	-1.2
	Best	N/A	-0.5

This table may be reformatted provided the side-by-side comparison of options is retained	**1. Business as usual (baseline)**	**3. Preferred way forward (if not do-minimum)**
Public sector financial costs (with brief description, including ranges)	0	The public sector is expected to incur costs as a result of the legislation enabling a greater number of corporate prosecutions, increasing the burden on law enforcement and the CJS. This cost has not been quantified due to a lack of evidence for the likely scale of the increase. Through consultation with the CPS and SFO, additional court cases are expected to be low, and any additional costs are expected to be modest.
Significant un-quantified benefits and costs (description, with scale where possible)	N/A	The main unmonetised benefit of this reform is that it is expected to reduce crime. This is the primary benefit as the greater risk of prosecution, and the corresponding penalties, will impact on the corporates' incentives to commit crimes through an expected increase in deterrence. The reforms will significantly improve the ability to cooperate with international partners in high-profile cases against global organisations.
Key risks (and risk costs, and optimism bias, where relevant)	…	There is a risk that more people than expected are required to familiarise themselves with material, or that they read slower.
Results of sensitivity analysis	N/A	Whilst Fraud is not an offence in scope of this legislation reform, for lack of more suitable data on relevant crime types, a breakeven analysis of the identification doctrine reform's monetised costs was conducted against the unit cost of fraud to provide an indicative sense of scale. In a central scenario with monetised costs of £0.50 million, the identification doctrine would have to prevent 348 fraud offences to recover costs and breakeven (116 and 858 frauds in the low and high scenarios respectively).

Proposal 2: Suspension of Internet Protocol Addresses and Internet Domain Names

Price base year: 2024-25

PV base year: 2024/25

This table may be reformatted provided the side-by-side comparison of options is retained		**0. Business as usual (baseline)**	**4. Preferred way forward (if not do-minimum)**
Costs (£m)	Low	0	0.38
	High	0	0.42
	Best	0	0.40
(Distinguish between setup and ongoing costs, as well as private/public costs)		Under the 'Do nothing' option, the majority of domestic domain suspensions would be handled under the existing voluntary relationships, but international domain suspensions and a minority of domestic cases would not be covered.	Estimated familiarisation costs to the public sector lie in the range of l: £130, c: £487 , h: £909 Annual LE wage costs attributable to increase in suspensions: l: £0.24m, c: £0.25m, h: £0.26m; Judicial costs for signing off suspensions: l: £0.14m, c: £0.14m, h: £0.15m Private domain registry and registrar wage costs attributable to increase in suspensions: l: £2,000, c: £5000, h: £7,000
Benefits (£m)	Low	0	0
	High	0	0
	Best	0	0
(Distinguish between setup and ongoing benefits, as well as private/public benefits			
Net present social value (£m)	Low	N/A	-0.42
	High	N/A	-0.38
	Best	N/A	-0.40

This table may be reformatted provided the side-by-side comparison of options is retained	**1. Business as usual** **(baseline)**	**3. Preferred way forward** **(if not do-minimum)**
Public sector financial costs (with brief description, including ranges)	0	Estimated familiarisation costs to the public sector, are negligible, and lie in the range of £130 to £487 with a central estimate of £909 in year 1 only. Total public ongoing costs of the proposal are estimated to lie in a range of **£0.38** to **£0.41 million** with a central estimate of **£0.40 million**, (10-year PV). Public ongoing costs comprise officer and judicial time to process suspensions, using existing staff.
Significant un-quantified benefits and costs (description, with scale where possible)	N/A	The increase in domain name/IP address suspensions will lead to a reduction in cyber enabled fraud and remove nodes in criminal enterprises for cyber enabled fraud, breakeven analysis is undertaken in the benefits section to illustrate the possible scale of benefits. Increased confidence in UK government and ability to police online activity.
Key risks (and risk costs, and optimism bias, where relevant)	…	Assumption that legislation to allow law enforcements agencies to apply to the courts for international suspensions will not impact existing voluntary relationships with UK domain and IP address providers. Two hours of NCA/ LE processing time for each suspension split between officer and manager. Assumption that domain name/ IP address suspensions lead to the avoidance in cyber fraud offences, however this is not monetised due to uncertainty. Risk of displacement, domain name/ IP addresses suspended may lead to harmful domain names/IP addresses being created elsewhere.

Results of sensitivity analysis	N/A	For fraud, breakeven analysis estimates that the policy would have to result in, over ten years, 270 avoided fraud offences to cover costs in the central case, or 26 avoided cases per year. The number of offences avoided decreases to 258 in the low case and increases to 281 in the high case. Separately, for cyber crime, breakeven analysis estimates that the policy would have to result in, over ten years, 1110 avoided cyber crime offences to cover costs in the central case, or 111 avoided cases per year. The number of offences avoided decreases to 1063 in the low case and increases to 1158 in the high case.

Proposal 3: Ban the supply or possession of devices known as 'SIM farms' in the UK

Price base year: 2025/26

PV base year: 2025/26

This table may be reformatted provided the side-by-side comparison of options is retained		**0. Business as usual (baseline)**	**4. Preferred way forward (if not do-minimum)**
Costs (£m)	Low	0	0.01
	High	0	0.04
	Best	0	0.02
(Distinguish between setup and ongoing costs, as well as private/public costs)			All estimated costs are costs familiarisation costs that fall on the public sector.
Benefits (£m)	Low	0	0
	High	0	0
	Best	0	0
(Distinguish between setup and ongoing benefits, as well as private/public benefits			
Net present social value (£m)	Low	N/A	-0.04
	High	N/A	-0.01
	Best	N/A	-0.02

This table may be reformatted provided the side-by-side comparison of options is retained	**1. Business as usual (baseline)**	**3. Preferred way forward (if not do-minimum)**
Public sector financial costs (with brief description, including ranges)	0	Estimated familiarisation costs to the public sector range between £0.01m to £0.04m with a best estimate of £0.02m. These costs arise from Border Force Staff familarising themselves with the guidance instead of completing regular daily work.
Significant un-quantified benefits and costs (description, with scale where possible)	N/A	The main un-quantified benefit is from the expected reduction in the level of fraud and 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. This benefit is unmonetised as the extent to which the SIM farm ban will reduce the volumes and harm of fraud is unknown.
Key risks (and risk costs, and optimism bias, where relevant)	…	The key analytical risk lies in lack of monetised analysis. Limitations in data and evidence meant this was not possible. 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. From extensive engagement with legitimate suppliers this risk is expected to be low. There is a risk that the proposed ban may displace criminals to other methods of committing fraud. 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. The risk is therefore that the benefits may not be as large as expected, but would still outweigh the costs of displacement.
Results of sensitivity analysis	N/A	A breakeven analysis of fraud against individuals therefore suggests that the legislation would only need to avoid 25 frauds to recover the monetised costs in the high scenario.

Evidence base

Proposal 1: Reform the Identification Doctrine

General assumptions and data

241. The analysis is based on the following general assumptions:

    a. 2025/26 to 2034/35, a 10-year appraisal period: The analysis assumes that the measures come into force in 2025 and costs and benefits arise from that point onwards.

    b. 2025/26 price year and 2025/26 price base year.

    c. 3.5 per cent discount rate per the Green Book (2022)[15].

242. Key data sources used for this analysis:

    a. Business Population Estimates 2022[16] used to inform numbers of organisations in scope.

    b. Annual Survey of Hours and Earnings 2023[17] used to inform wage costs.

    c. Readingsoft.com used to calculate familiarisation costs.

COSTS

Set-up costs

Private sector familiarisation costs

243. Larger organisations are the focus of the analysis as smaller organisations are more likely to have one or a low number of directors with responsibility who will be more easily identifiable to hold the corporate liable. The policy intends to level the playing field between smaller and larger organisations by making it easier to attribute blame to a large company with many directing minds across varied business functions. Therefore, upon introduction of the reform, it is assumed that large organisations will take steps to familiarise with it. This analysis assumes that company secretaries in large organisations will familiarise themselves with the reform.

244. The length of the legislation and the number of people required to familiarise themselves with it are Home Office estimates. The length is assumed to be 1000, 2000 and 3000 words in the low, central and high scenarios, respectively.

245. With it assumed that only the largest organisations are in scope of this legislation, the number of organisations is taken from the Business Population Estimates (BPE) and the staff required to read the guidance is assumed by the Home Office.

Table 1: Organisations in scope of identification doctrine reform

Organisation size	Companies and Partnerships	People required to read
Large	11,038	4
Largest	11,018	5

Source: BPE and Home Office internal assumptions

246. The analysis uses a median wage of £24.96 per hour for a company secretary from 2023 ASHE data, which is then uplifted by 22 per cent to reflect the non-wage costs using Eurostat

figures to reflect the marginal product of labour[18]. This figure is then adjusted to the 2025/26 price year using the GDP deflator, resulting in a total hourly cost of £33.88.

247. To estimate the familiarisation cost of this measure, the Reading Soft calculator was used to estimate the time taken to read the legislation. This was then multiplied by the cost of time and the number of people required to read the legislation.

248. The identification doctrine familiarisation costs are estimated to be between **£0.2 million to £1.2 million**, with a best estimate of **£0.5 million** (2025/26 prices) in year 1 only. These are presented in Table 3 by organisation size.

Table 2, Total identification doctrine familiarisation costs by organisation size, £ million (2025/26 prices), PV Base 2025/26.

Organisation size	Low	Central	High
Large	0.07	0.22	0.55
Largest	0.09	0.28	0.69
Total	**0.2**	**0.5**	**1.2**

Source: Home Office internal estimates, 2024

Non-monetised set-up costs

249. It is expected that costs to SMEs will be negligible. As SMEs can currently be effectively prosecuted under the current identification doctrine, it is unlikely this measure will have an impact on SMEs.

As a part of their day-to-day business, SMEs may read advice issued by trade bodies or industry organisations however it is expected that this opportunity cost is negligible.

Public sector

250. No public sector set-up costs have been identified

Total set-up costs

251. Total set-up costs are estimated in a range of **£0.17 million to £1.24 million**, with a best estimate of **£0.50 million** (2025/26 prices) in year 1 (see Table 2).

Table 3, Total set-up costs for the identification doctrine, £ million (2025/26 prices), year 1 only, 2025

	Low	High	Best
Identification doctrine	0.2	1.2	0.5

Source: Home Office internal calculations, 2024.

Ongoing costs Private sector

252. No ongoing costs have been identified.

253. There are unlikely to be additional costs to business because:

a. Organisations can already be prosecuted under the common law model, but the reform means a greater number of cases could see a higher likelihood of successful prosecution.

b. The identification doctrine attributes liability to an organisation for an existing criminal offence which organisations should be familiar with on the introduction of that offence into law.

c. Organisations may incur costs if they choose to put measures in place to increase transparency and control with senior management, such as awareness training, to

minimise their liability if criminal conduct takes place. However, there is no requirement in the legislation for them to do so.

Public sector

254. The public sector is expected to incur costs as a result of the legislation enabling a greater number of corporate prosecutions, increasing the burden on law enforcement and the CJS. This cost has not been quantified due to a lack of evidence for the likely scale of the increase. Through consultation with the CPS and SFO, additional court cases are expected to be low, and any additional costs are expected to be modest.

255. It is likely that corporate prosecutions will be dealt with by a Deferred Prosecution Agreement and, where corporate prosecution is desirable, the corporation might be tied to the same proceedings as the manager.

Total costs

256. Total costs are estimated in a range of **£0.17 million to £1.24 million**, with a best estimate of **£0.50 million** (2025/26 prices) in year 1. There are unlikely to be additional ongoing costs.

Benefits

257. The identification doctrine applies to all crimes. The benefits are all non-monetised as the Home Office has so far not been able to source well-evidenced estimates for the number and type of criminal acts that this legislation will prevent. This is because the data on failed prosecutions, due to the challenges under the current common law identification doctrine, cannot easily be identified from CPS records.

258. It would be costly to collect data on all potential cases the identification doctrine could apply to, as this would require consultation with users of any law in England and Wales. Consequently, this IA only provides a qualitative assessment of benefits.

259. This legislation aims to reduce the incidence of corporate criminality through behavioural and cultural changes. This reform will help to enable the prosecution of low incidence, high harm offences.

260. The main benefit is that a clearly formulated legal test for the attribution of crimes will enable corporates to be prosecuted if they break the law. The benefits this will bring are presented below.

Non-monetised benefits

261. This reform is expected to reduce crime. This is the primary benefit as the greater risk of prosecution, and the corresponding penalties (detailed below), will impact on the corporates' incentives to commit crimes. This is expected to result in deterrence. The penalties can include:

- Corporate criminal conviction will result in a fine.
- Criminal convictions can exclude organisations from public procurement processes and domestic and international contracts. This can have negative impacts on investors, other employees, and even customers, should the corporate suffer financially because of the conviction.
- Beyond a fine, there are other available methods of punishing wrongful corporate behaviour such as granting a Serious Crime Prevention Order, implementing a monitor in a Deferred Prosecution Agreement, seeking a disgorgement of profits, or making a confiscation order to pay back the proceeds of crime. All of these are expected to increase deterrence and result in reduced crime.

262. The reform can increase the UK's ability to support international partners. In some cases, it has not been possible for the UK to bring parallel proceedings (for example in support of the US) to address corporate financial misconduct. The reforms will significantly improve the ability to cooperate with international partners in high-profile cases against global organisations. This may increase international and public confidence in the UK's CJS, and increase deterrence.

Value for Money

263. To be considered value for money a policy must meet its strategic objectives. Under the current legislation, multiple senior managers within a large organisation could commit corporate crimes without consequence thanks to complex organisational structures which make it difficult to attribute blame. By increasing the ability to prosecute large organisations in such instances, the reform to the identification doctrine is anticipated to meet its strategic objective of reducing corporate criminal activity. This is strengthened by the identification doctrine imposing the threat of criminal conviction and an unlimited fine, enhancing the deterrence effect. The progress of the policy against its strategic objectives will be a specific evaluation question in the post implementation review.

264. The identification doctrine has a negative NPSV of between -£0.17 million and -£1.24 million (Price Base 2025/26; PV Base 2025/26), this is since the cost of staff familiarising with the document has been monetised, but all the benefits are qualitative. Consequently, the NPSV in this Options Assessment cannot be considered indicative of the overall value for money for society. The benefits are all non-monetised as it has not been possible to obtain sufficient data for the number and type of criminal acts that this legislation could prevent as well as the resulting harms. This is because data on failed prosecutions cannot easily be identified from CPS records due to the challenges under the common law identification doctrine. The strategic case highlights that it would be costly to collect data on all potential cases the identification doctrine could apply to, as this would require consultation with users of any law in England and Wales. Whilst monetisation is not possible, break-even analysis can be used to assess the number of crimes that would have to be avoided to cover the monetised familiarisation cost. However, it is challenging to apply a suitable unit cost of crime to compare against the policy's monetised costs.

265. Referring to the Economic and Social Costs of Crime (which considers crimes perpetrated by individuals, not corporations), the department has determined that in the absence of well evidenced data on which crime types maybe avoided the cost of Fraud provides the best available proxy for an indicative breakeven analysis of the identification doctrine reform[19]. This is despite the identification doctrine applying legislation to cover all offences besides economic crimes, which had already been covered in ECCT Act 2023.

266. For lack of more suitable data on relevant crime types, a breakeven analysis of the identification doctrine reform's monetised costs against the unit cost of fraud is as follows:

- From The Economic and Social Costs of Crime, the unit cost of Fraud is estimated to be £1,290 in 2015/16 prices, noting that this reflects the cost of fraud against individuals rather than businesses[20]. From this figure the anticipation component is deducted as anticipation is assumed to be incurred before the crime takes place, and won't be impacted by any reduction to the volume of crime attributable to the identification doctrine. The unit cost of Fraud excluding anticipation is £1,070 in 2015/16 prices.
- Uplifting this value to 2025/26 prices using the GDP deflator gives an average loss of £1,450.25.

- In a central scenario with monetised costs of £0.50 million, the identification doctrine would have to prevent 348 fraud offences to recover costs and breakeven (116 and 858 frauds in the low and high scenarios respectively).

267. The department reiterates that this breakeven analysis is intended only to provide an indicative sense of scale. Whilst Fraud is not an offence in scope of this legislation reform, this approximate analysis helps demonstrate that only a relatively small number of offences must be prevented to recover the monetised costs of the policy. If the identification doctrine prevents non-economic offences that fall in scope (which may be of higher value when perpetrated by corporations rather than individuals) then the policy could breakeven and potentially deliver considerable societal benefits.

Place based analysis

268. No distributional effects are expected.

Impact on small and micro-businesses

269. The identification doctrine will apply to corporations and partnerships. Previously, small and micro-organisations were at a disadvantage as they are more likely to have one or a low number of directors with responsibility for and oversight of everything in the corporation that are more easily identifiable to hold the corporate liable. This is an unfairness in the operation of the law. The new model intends to level the playing field by better applying the identification doctrine in instances where a company is large with multiple directing minds across varied business functions.

Proportionality

270. Costs arising from this measure are expected to only fall to familiarisation for companies and partnerships. As the legislation is not expected to have any significant impacts on government, businesses or the general public, the limited level of analysis is proportionate.

Proposal 2: Suspension of Internet Protocol Addresses and Internet Domain Names

General assumptions and data

271. The general assumptions used in this IA are as follows. The appraisal period for measuring the impacts is 10 years, starting in 2025/26. A 3.5 per cent annual social discount rate is used, as per HMT Green Book guidance. Annual costs and benefits are in 2025/26 prices. All costs and benefits are relative to the **Option 0: 'Do nothing'.** The number of expected suspensions for domains and IP addresses, domestically and internationally are provided by the NCA, NPCC and HMRC, based on the number of historic cases in which the power would have been used or how many cases have been refused due to lack of judicial backing.

Table 4: Expected number of suspension cases in which the power will be used, yearly.

	NCA	NPCC	HMRC	Total
Domestic domain	3 to 12	0	0	**3 to 12**
International domain	9 to 37	458	3 to 5	**470 to 500**
Domestic IP address	1	0	0	**1**
International IP address	3	0	1	**4**

Source: NCA, NPCC, HMRC

COSTS

Set-up costs

Public sector familiarisation costs

272. There are familiarisation costs to the public sector expected to occur in the first year of appraisal, impacting the NCA and LE. These will be incurred by staff members who will need to familiarise themselves with the proposal.

273. It is assumed that the staff members will have to read 1,000 words of materials relating to the operation of the Scheme (a range of 800 to 1,200, some using a screen, others using paper copies).

274. Hourly cost is taken from the ONS Annual Survey of Hours and Earnings (ASHE) 14.5a 2022[59] – police officers: sergeant and below, and senior police officers – and uplifted by Eurostat public non-wage costs. It is estimated that 50 police officers and senior police officers will need to familiarise themselves with the policy.

275. The values used to estimate familiarisation costs to staff members is presented in Table 5 as given:

Cost = reading time x wage x volume of staff

Table 5: Familiarisation Costs to the public sector, 2024/25 prices (£).

	Low	Central	High
Number of Words			
Paper	800	1000	1200
Screen	800	1000	1200
Familiarisation Cost			
Paper	66	230	427
Screen	64	257	482
Total Familiarisation Cost	**130**	**487**	**909**

Source: Home Office Internal Analysis, 2022. Figures may not sum due to rounding.

276. Estimated familiarisation costs to the public sector lie in the range of **£130 to £909 with a central estimate of £487** in year 1 only.

Private sector familiarisation costs

277. Familiarisation costs to business are not expected as domain and IP address registries perform suspensions as part of their business as usual operations.

Ongoing and total costs

Public sector ongoing costs

278. Introduction of a power to suspend domain names and IP addresses will incur a cost to the NCA, HMRC and LE agencies of Full Time Equivalent (FTE) time required to process each suspension, reported in Table 6. This is an opportunity cost to these agencies as existing staff will be processing these suspensions.

279. The time reported to process a suspension is estimated by the NCA, based on experience of similar procedures. The number of international suspensions to be performed is estimated by the NCA using historical cases when such a power would have been used. This time taken is assumed to be equal for domain name and IP address suspensions, both

[59] ONS Earnings and hours worked, occupation by four-digit SOC: ASHE Table 14: https://www.ons.gov.uk/employmentandlabourmarket/peopleinwork/earningsandworkinghours/datasets/occupation4digitsoc2010ashetable14

internationally and domestically. The NCA estimate the time taken to process each suspension over both officer and senior police officer signoff to be two hours, an assumption of 80 per cent officer time, 20 per cent senior officer sign off time is applied. Estimated number of additional suspensions (Table 4) will be between 478 and 517 a year, a central case of 498 is taken. Hourly cost is taken from ASHE14.5a 2022 – police officers: sergeant and below, and senior police officers - and uplifted by Eurostat public non-wage costs.

280. **Table 6, Annual LE wage costs attributable to increase in suspensions, 2024/25 prices.**

	Low	Central	High
Time to Process Each Suspension (hr) - Officer	1.6	1.6	1.6
Time to Process Each Suspension (hr) - Manager	0.40	0.40	0.40
Estimated Increase in number of Domain Suspensions TOTAL	478	497.5	517
Estimated Time to Process Increase in Suspensions (hours)	956	995	1034
Wage/hr (£) Officer	27.40	27.40	27.40
Wage/hr (£) Manager	38.36	38.36	38.36
Annual Wage Cost to Process Increase in Suspensions (£)	28,289	29,443	30,597
10-year cost, PV (£)	243,504	253,438	263,371
10-year cost, PV, £m	0.24	0.25	0.26

Source: Home Office Internal Analysis, 2022. Figures may not sum due to rounding.

281. Total public ongoing costs to the NCA, LE and HMRC of the proposal are estimated to lie in a range of £0.24 to £0.26 million with a central estimate of £0.25 million, (10-year PV).

282. Introduction of a power to seize suspend domain names and IP addresses will also incur a cost for judicial signoff of each suspension, reported in Table 7. It is assumed the time taken for a judge to sign off each suspension will be equal to the time taken for a senior police officer to sign off a suspension, and that courts do not have to sit.

283. Hourly cost is calculated from Ministry of Justice: Judicial Salaries by Salary Group (effective 1 April 2022)[60], salary group 7 for District Judge (Magistrates Court), ASHE 14.9a 2022[61]: average hours worked by Barristers and Judges, uplifted by Eurostat public non-wage costs.

[60] Judicial salary schedule 2022 to 2023.pdf (publishing.service.gov.uk), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1116006/judical-salary-schedule-2022-23.pdf

[61] Earnings and hours worked, occupation by four-digit SOC: ASHE Table 14 - Office for National Statistics (ons.gov.uk), https://www.ons.gov.uk/employmentandlabourmarket/peopleinwork/earningsandworkinghours/datasets/occupation4digitsoc2010ashetable14

Table 7: Judicial costs for signing off suspensions, 10 years

	Low	Central	High
Time to sign off each suspension (hours)	0.4	0.4	0.4
Wage/hr (£) Judge	85.1	85.1	85.1
Estimated Increase in # of Domain Suspensions, yearly	470	485	500
Annual Wage Cost to Process Increase in Suspensions (£)	16,005	16,516	17,027
10-year cost, PV (£)	137,768	142,165	146,561
10-year cost, PV, £m	0.14	0.14	0.15

Source: Home Office Internal Analysis, 2022. Figures may not sum due to rounding.

284. Total public judicial ongoing costs of the proposal are estimated to lie in a range of **£0.14 million** to **£0.15 million** with a central estimate of **£0.14 million**, (10-year PV).

Table 8: Total public ongoing costs, 10 years

	Low	Central	High
Total ongoing costs, PV, £	381,142	395,115	409,024
Total ongoing costs, PV, £m	0.38	0.40	0.41

Source: Home Office Internal Analysis, 2022. Figures may not sum due to rounding.

285. Discussions with LE suggest that current ticketing systems used to record and track the progress of suspension requests can continue to be used to deal with the additional requests allowed by this legislation. It is also not expected that this power will cause additional equipment burden in addition to what is already in existence under the voluntary regime.

286. The Home Office do not expect additional costs to be incurred by LE due to the international coordination element between the UK and targets of the orders. This is because LE already coordinates with international partners under the voluntary framework, and in general this is part of the business as usual for modern policing since online crime easily cuts across borders. For example, in 2024 the NCA worked with 10 countries to disrupt LockBit, a cyber crime group.[62]

287. Total public ongoing costs of the proposal are estimated to lie in a range of **£0.38** million to **£0.41 million** with a central estimate of **£0.40 million**, (10-year PV).

Private sector ongoing costs

288. The majority of domestic suspensions will be dealt with under existing voluntary relationships; however a minority will come into scope of the measure following ministerial consideration.

289. Based on the number of historic cases in which the power would have been used or how many cases have been refused due to lack of judicial backing, the NCA expect between 3 and 12 domestic domain suspensions and 1 domestic IP address suspension, HMRC and NPCC do not expect any domestic domain or IP address suspensions.

290. The NCA estimate the time taken to process each suspension over both officer and senior police officer signoff to be two hours, an assumption of 80 per cent officer time, 20 per cent senior officer sign off time is applied. This assumption is carried over to business for two hours of total time taken to process a suspension, split between domain registry and

[62] https://www.nationalcrimeagency.gov.uk/news/nca-leads-international-investigation-targeting-worlds-most-harmful-ransomware-group

registrar employees and managers and an 80 per cent 20 per cent time requirement, respectively.

291. Hourly cost is taken from ASHE 14.5a 2022[63] – cyber security professionals and IT project manager - and uplifted by Eurostat private non-wage costs.

292. Possible costs to internationally based registries and registrars are not captured due to lack of impact in the UK.

Table 9, Annual private domain registry and registrar wage costs attributable to increase in suspensions, 2024/25 prices

	Low	Central	High
Time to Process Each Suspension (hr) – Employee	1.6	1.6	1.6
Time to Process Each Suspension (hr) – Manager	0.4	0.4	0.4
Estimated Increase in number of Domain Suspensions TOTAL	4	8.5	13
Wage/hr (£) Employee	29.48	29.48	29.48
Wage/hr (£) Manager	36.59	36.59	36.59
Annual Wage Cost to Process Increase in Suspensions (£)	247.23	525.36	803.49
10-year cost, PV, £	2,128	4,522	6,916
10-year cost, PV, £m	0.00	0.00	0.01

Source: Home Office Internal Analysis, 2022. Figures may not sum due to rounding.

293. Present value costs to business over 10 years could fall between **£2,000 (£0.00 million)** in the low case and **£7,000 (£0.00 million)** in the high case with a central estimate of **£5,000 (£0.00 million)**.

Total Costs

294. Total costs of the scheme are estimated to lie in a range of £0.38 million to £0.42 million with a central estimate of £0.40 million (PV over 10 years).

295. These costs are made up of ongoing agency and judicial costs of processing and signing off suspensions and year one familiarisation costs to the public sector and ongoing costs of suspending domain names and IP addresses for industry.

BENEFITS

Non quantifiable benefits

296. Benefits have not been calculated as it is not possible to link the outcome of a domain name and IP address suspension to impact in terms of reduced criminality due to a selection of factors. Lack of knowledge of when most of the harm occurs in the lifecycle of the domain and IP address, backfill of new domains and IP addresses, and variation in harm in domains and IP addresses. As such, breakeven analysis has been performed to give a scale of the number of offences that would have to be avoided for the program to cover its costs.

297. Whilst not proven officially, evidence suggests domain suspensions have a positive impact on internet safety. The NSCS takedown service works with internet hosts to remove dangerous websites. In 2022, the NCSC removed 2.1 million cyber-enabled commodity

[63] ONS Earnings and hours worked, occupation by four-digit SOC: ASHE Table 14: https://www.ons.gov.uk/employmentandlabourmarket/peopleinwork/earningsandworkinghours/datasets/occupation4digitsoc2010ashetable14

campaigns, during this time, the number of fake UK government phishing scams reduced from 13,000 to 6,000, a 54 per cent decrease.

298. Although the estimated increase in the number offences avoided cannot be reliably estimated, there will be an increase and consequently a monetary benefit in terms of crime avoided.

Breakeven Analysis

299. As it is not possible to reliably estimate the increase in fraud offences avoided, breakeven analysis is provided, to estimate the number of avoided fraud or computer misuse act offences that are required to be avoided to cover the costs outlined above. One suspension can lead to multiple fraud offences avoided, and the expected number of suspensions outlined in Table 4 above can feasibly lead to the number of fraud or cyber crime offences set out in Table 8 below.

300. Unit costs for the consequence of and response to Fraud and Cyber Crime offences are taken from the Home Office, Economic and Social Costs of Crime, 2018, inflated to 2024/25 values.

Table 7: Home Office, Economic and Social Costs of Crime, 2018, Fraud and Cyber Crime, 2024/25 Prices (£)

Crimes	**Estimated unit costs of crime (2015/16 prices)**			
	Consequence	Response	Total unit cost: consequence, and response	2025/26 prices
Fraud	720	130	850	1036
Cyber crime	520	0	520	634

Source: Home Office Internal Analysis, 2022.

Table 8: Number of fraud or cyber crime offences avoided to breakeven over the 10-year appraisal period

	Fraud	Cyber Crime
Low	258	1063
Central	**270**	**1110**
High	281	1158

Source: Home Office Internal Analysis, 2022. Figures may not sum due to rounding.

301. Table 8 sets out the number of fraud offences required to breakeven, and separately the number of Cyber crime offences required to breakeven.

302. For fraud, breakeven analysis estimates that the policy would have to result in, over ten years, 270 avoided fraud offences to cover costs in the central case, or 26 avoided cases per year. The number of offences avoided decreases to 258 in the low case and increases to 281 in the high case.

303. For cyber crime, breakeven analysis estimates that the policy would have to result in, over ten years, 1110 avoided cyber crime offences to cover costs in the central case, or 111 avoided cases per year. The number of offences avoided decreases to 1063 in the low case and increases to 1158 in the high case.

NPSV: monetised and non-monetised costs and benefits of each shortlist option (including administrative burden)

NPSV, BNPV, EANDCB

Table 9, Summary costs and benefits (PV) 10 years, 2025/26

Summary	Low	Central	High
Costs			
Total Set up Costs (£)	128	482	899
Total Ongoing Costs (£m)	0.38	0.40	0.42
Total Costs (£m)	**0.38**	**0.40**	**0.42**
Benefits			
Ongoing Benefits (£m)	0	0	0
Total Benefits (£m)	**0**	**0**	**0**

Source: Home Office Internal Analysis

304. Total costs of the scheme are estimated to lie in a range of £0.38 to £0.42 million with a central estimate of £0.40 million above baseline (PV over 10 years).

Table 10, NPSV, BNPV and EANDCB, 2025/26

	Low	Central	High
NPSV (£m)	-0.42	-0.40	-0.38
BNPV (£)	**-6,916**	**-4,522**	**-2,128**
EANDCB (£)	**247**	**525**	**803**

Source: Home Office Internal Analysis, 2022. Figures may not sum due to rounding.

305. There are no monetised benefits, and therefore the NPSV has a low estimate of -£0.42 million (corresponding to the high cost scenario), a central estimate of -£0.40 million, and a high estimate of -£0.38 million (corresponding to the low cost scenario) above baseline (PV over 10 years).

Value for money (VfM)

306. Whilst no benefits can be attributed to the policy due to uncertainty in impact attributable to domain name and IP addresses suspensions, costs are low and breakeven analysis shows that very few crimes need be avoided for reduced harms to cover costs.

307. The policy is not assumed to impact legitimate small or micro businesses over, and above costs incurred from business as usual.

308. There should be little or no cost burden for a registry or registrar acting upon the order. The processes can generally be automated and there is an existing process for ICANN to waive the nominal fee they charge registries upon the creation of a domain name, when the action is in support of a court order issued to LE.

309. The Home Office does not consider that there is any requirement for the registry/registrar to be able to refuse to comply with the order on costs grounds. Similarly, the department has sought to limit the impact of the cost implications for businesses of having to purchase new IP addresses by restricting the length of time for which an order is made and ensuring the IP is retained by the Local Internet Registries for future use.

Costs and benefits to business calculations

Table 11, Annual private domain registry and registrar wage costs attributable to increase in suspensions, 2024/25 prices

	Low	Central	High
Time to Process Each Suspension (hr) – Employee	1.6	1.6	1.6
Time to Process Each Suspension (hr) – Manager	0.4	0.4	0.4
Estimated Increase in # of Domain Suspensions TOTAL	4	8.5	13
Wage/hr (£) Employee	29.48	29.48	29.48
Wage/hr (£) Manager	36.59	36.59	36.59
Annual Wage Cost to Process Increase in Suspensions (£)	247.23	525.36	803.49
10-year cost, PV, £	2,128	4,522	6,916
10-year cost, PV, £m	0.00	0.00	0.01

Source: Home Office Internal Analysis, 2022. Figures may not sum due to rounding.

310. Present value costs to business over 10 years could fall between **£2,000 (£0.00 million)** in the low case and **£7,000 (£0.01 million)** in the high case with a central estimate of **£4,000 (£0.00 million)**.

311. Business Net Present Value Present over 10 years could fall between **-£2,000 (-£0.00 million)** in the low case and **-£7,000 (-£0.01 million)** in the high case with a central estimate of **-£4,000 (-£0.00 million)**.

312. The Equivalent Annual Net Direct Costs to Business (EANDCB) could fall between £247 in the low case and £803 in the high case with a central estimate of £525.

The policy is not assumed to have a disproportionate impact legitimate to small or micro businesses over, and above costs incurred from business as usual.

Costs and benefits to households' calculations

313. No costs or benefits calculated.

314. The increase in domain name IP address suspensions will lead to a reduction in cyber enabled fraud and remove nodes in criminal enterprises for cyber enabled fraud, breakeven analysis is undertaken in the benefits section to illustrate the possible scale of benefits to households and individuals.

315. Benefits have not been calculated as it is not possible to link the outcome of a domain name and IP address suspension to impact in terms of reduced criminality due to a selection of factors. Lack of knowledge of when most of the harm occurs in the lifecycle of the domain and IP address, backfill of new domains and IP addresses, and variation in harm in domains and IP addresses. As such, breakeven analysis has been performed to give a scale of the number of offences that would have to be avoided for the program to cover its costs.

316. Although the estimated increase in the number offences avoided cannot be reliably estimated, there will be an increase and consequently a monetary benefit in terms of crime avoided.

Environment: Natural capital impact and decarbonisation

317. There are no environmental impacts associated with the policy option the Home Office are recommending taking forward.

Other wider impacts (consider the impacts of your proposals)

318. Increased confidence in the government and the ability to police online activity.

Risks and assumptions

319. Assumption that legislation to allow law enforcements agencies to apply to the courts for international suspensions will not impact existing voluntary relationships with UK domain and IP address providers.

320. Two hours of NCA/LE processing time for each suspension split between officer and manager.

321. Assumption that domain name/ IP address suspensions lead to the avoidance in cyber fraud offences, however this is not monetised due to uncertainty.

322. Risk of displacement, domain name/ IP addresses suspended may lead to harmful domain names/IP addresses being created elsewhere.

Impact on small and micro-businesses

323. The policy is not assumed to have a disproportionate impact legitimate to small or micro businesses over, and above costs incurred from business as usual.

324. The Home Office does not expect the proposal to increase the number of IP and domain name suspensions for domestic SMBs to increase, instead adjusting the way that LE will approach SMBs for the suspensions.

325. SMB domain registrars already suspend malicious domain and IP addresses as part of their business as usual activities, the Home Office does not expect that any new processes or greater employee capacity will be required as a result of these measures.

326. Domestic uses of the power are expected to be low as voluntary relationships will still be used when possible, in the high case only 12 domestic domain suspensions and 1 domestic IP address suspension a year with an expected yearly cost of under £1000 across all businesses.

Proposal 3: Ban the supply or possession of devices known as ‘SIM farms’ in the UK

General assumptions and data

327. While efforts have been made to understand the costs and benefits to all affected groups, most 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. Due to an absence 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.

328. The general assumptions are as follows:

- 2025/2026 to 2034/2035, a 10-year appraisal period: The analysis assumes that the measures come into force in 2025/2026 and costs and benefits arise from that point onwards.

329. A 3.5 per cent annual social discount rate is used[64].

- Annual costs and benefits are in 2025/26 prices.
- Present values are in 2025/26 prices.

COSTS

Set-up costs

Private Sector

330. Minor familiarisation costs to the private sector are expected as distributors, suppliers and users will need to familiarise themselves with the legislation and put in place processes for 'reasonable checks' going forwards. An absence of evidence means this has not been quantified.

331. 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

Familiarisation Costs

Border Force

332. Economic opportunity cost of staff familiarising themselves with the guidance instead of completing regular daily work.

333. One-off familiarisation costs are expected as the change in legislation will mean that Border Force staff will have to familiarise themselves with how the legislation will be implemented. This analysis assumes that all Border Force staff will be required to familiarise themselves with any relevant guidance produced to support the policy. The familiarisation costs should occur only in year 1 after the implementation of the legislation.

334. Documentation associated with this legislative change, including the legislative provisions, and Explanatory Notes to any future Act, are expected to be 500 to 1,000 words long. This is standard for non-assigned matters without complications. The familiarisation cost is calculated by multiplying time to read by the labour cost of each Border Force staff.

335. Table 11 shows the total number of Border Force operational staff that will need to familiarise themselves with the guidance in the low central and high scenarios.

[64] The Green Book (2022) - https://www.gov.uk/government/publications/the-green-book-appraisal-and-evaluation-in-central-governent/the-green-book-2020

Table 11: Border Force Staff by Grade and Median Hourly Labour Cost[65] (2025/26 prices)

Staff	Staff in Scope - FTE	Staff in Scope - Headcount	Weighted Average Hourly Labour Cost (£)
Senior	450	459	58.63
Non-Senior	9,539	10,069	25.70
Total	9,989	10,528	27.26

Source: Home Office internal estimates for staff in scope, 2023. Accompanying weighted average hourly labour cost uplifted to 2025/26 prices.

336. A reading time calculator has been used to estimate how long it would take an individual to read the guidance, with reading speeds of 200, 300 and 400 words per minute used for the low, central, and high scenarios, respectively[66]. This provided a central estimate of 2.5 minutes.

337. Multiplying the anticipated time taken to read the guidance by total hourly earnings, and then scaling this to the total number of Border Force Staff who must familiarise with the guidance gives the total familiarisation cost. This is presented in Table 12.

Table 12: Border Force Staff Familiarisation Costs (2025/26 prices)

	Total Time (hours)	Hourly Earnings (£)	Number of Officers	Total Cost (£)
Low	0.02	27.26	9,989	5,445
Central	0.07	27.26	9,989	19,058
High	0.13	27.26	9,989	35,394

Source: Home Office internal estimates, 2024

Training Costs

338. The College of Policing ensure that all new legislation is incorporated into the national policing curriculum as a matter of course and falls within existing budgets. The additional public cost of training for this policy is expected to be negligible.

Ongoing and total costs

CJS Costs

339. CJS costs are expected to be negligible. As Home Office anticipate that there will be a relatively small number of cases per year for use and possession of SIM farms. Although the absence of evidence means it is not possible to provide a quantitative estimate.

340. The offence will carry the potential penalty of an unlimited fine in England or the maximum fine possible in Scotland. The offence will not carry the risk of custodial punishment.

Distributors, Suppliers and Users

341. The consultation on this policy included a call for evidence to collect information and data on the potential impacts of the SIM farm Ban. Due to the limited amount of evidence received, there remains uncertainties in relation to the impact of the proposal on businesses

[65] Staff FTE and headcount figures taken from internal Border Force HR data and covers all staff working within all functions of Border Force. Median hourly labour cost for Border Force staff taken from internal Border Force HR data and includes base pay and other non-pay staff expenditure such as pensions and national insurance. Border Force SCS Staff costs have been sourced from internal analysis

[66] Speed Reading Test Online (readingsoft.com): http://www.readingsoft.com/

and the costs associated with introducing and implementing the ban[67]. The options assessment presents the non-monetised impacts on business from the proposed action.

342. Businesses who distribute and supply these devices in the UK would need to demonstrate that they do so "in the course of business" and to undertake "reasonable customer checks" to ensure the customers they are supplying to intend to use the SIM farm for any of the exempt purposes outlined in the legislation.

343. It is possible that not all customers of UK based suppliers and distributors will fall under the proposed exemptions. If this is the case, the revenue of these businesses may fall as they cannot supply to the whole of their existing customer base.

344. The Home Office has conducted an extensive engagement process with legitimate distributors, suppliers and users of these devices and has not found any evidence to suggest that this would be the case and the likelihood and impact of this cost is expected to be low.

345. It is important to note that there is no evidence that the fraudsters using these devices are obtaining them from the legitimate UK suppliers, which will be exempted under the proposals.

BENEFITS

346. No set-up benefits are expected.

Ongoing and total benefits

Private Sector

347. 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 to 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.

348. 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.

349. 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.

350. 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.

[67] Preventing the use of SIM farms for fraud: government response: https://assets.publishing.service.gov.uk/media/655f3b45dcc6be000d5d1134/Government_Response_to_the_Consultation__Preventing_the_use_of_SIM_farms_for_fraud_.pdf

General public

351. 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.

352. 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.

353. Beyond the financial losses there are also wider harms and costs:

- Costs in anticipation: These are costs which are spent in defence from the fraud. For example, call blockers to prevent nuisance calls.
- Costs as a consequence: These are costs which are imposed on the victims and wider society as a result of the fraud. Beyond the financial harm this could include emotional harm felt by the victim, victim support costs and potential lost output if the victim took time off work.
- Costs in response: The costs of the police response to the fraud and any CJS costs.

354. 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.

NPSV, BNPV, EANDCB

355. The NPSV has a range from -£0.01 million, to -£0.04 million (PV), with a central estimate of -£0.02 million (PV 2025/26) over 10 years.

356. Due to limitations in the available data and evidence, the NPSV only includes familiarisation costs to Border Force. The low, central, and high estimates are driven by assumptions for the time taken to read the new guidance.

Table 13: Summary of monetised costs and benefits, £ million (PV) 2025/26 prices

Summary Costs	Low	Central	High
Total Set up Costs	0.01	0.02	0.04
Total Ongoing Costs	N/A	N/A	N/A
Total Costs	0.0	0.0	0.0
Total Benefits	0.0	0.0	0.0
NPSV	-0.01	-0.02	-0.04

Source: Home Office estimates, 2024

Value for money (VfM)

357. The policy is expected to meet both the strategic and policy objectives. 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.

358. Costs of implementing and running this policy to the private sector are expected to be low. The only identified costs to the public sector and familiarisation costs and CJS costs. The goal of the policy is to frustrate criminals' abilities to send mass fraudulent calls and texts, through limiting their ability to access SIM farms. The Home Office does not anticipate there will be many prosecutions for their use and possession and therefore, expects CJS costs to be negligible.

359. The extent to which the volumes and harm of fraud may be reduced due to this policy is currently unknown. If the policy does prove to be successful in reducing the harms of fraud, evidence suggests that the potential benefits may be significant.

360. To confirm this, an approximate Breakeven analysis demonstrates how few frauds the SIM Farm ban would need to avoid to recover the monetised costs, this is calculated whilst remembering that the true extent to which the ban will reduce the volume and harms of fraud is unknown.

361. Fraud is the most common CSEW recorded crime. The 2015/16 Economic and Social Cost of Crime estimates a unit cost of Fraud of £1,290 in 2015/16 prices. Note that this reflects only the cost of fraud against individuals. The impact of fraud on businesses is not reflected meaning that the true cost of fraud is likely to be higher. Note also that this cost estimate is used rather than calculating from the 2019/20 figure included in the Fraud Strategy . This is because the 2015/16 figure from the Economic and Social cost of crime can be more accurately broken down into its component parts.

362. The "anticipation" component of this cost is deducted as this is incurred before the crime takes place and therefore won't be impacted by any reduction to the volume of crime. The unit cost of fraud, excluding anticipation is therefore £1,070.

363. Uplifting this value to 2025/26 prices gives an average loss of £1,450.25.

364. The Economic and Social cost of Crime figure reflects fraud against individuals only, the impact of fraud against businesses is not reflected meaning that the total cost of fraud to the UK is likely significantly higher. A breakeven analysis of fraud against individuals therefore suggests that the legislation would only need to avoid 25 frauds to recover the monetised costs in the high scenario.

365. Whilst this Impact Assessment lists additional costs that cannot be monetised, it is not anticipated that these would significantly increase the number of frauds that would have to be avoided for the policy to break even.

366. Considering again the large scale of Fraud, any reductions in incidences of fraud attributable to this legislation could therefore yield significant societal benefits.

367. Since there are no monetisable benefits, no Benefit-Cost Ratio (BCR) has been calculated.

Place-based analysis

368. This measure will impact all UK-based companies equally and therefore will follow the geographical distribution of UK businesses.

369. Victims of fraud are spread mostly evenly across the country. According to the Crime Survey for England and Wales, adults in the East of England, Southeast of England and London are most likely to be victims of fraud (8.1 per cent, 8.8 per cent, and 7.5 per cent victimised respectively) and adults in the Northeast of England are the least likely to be victims at (3.8 per cent victimised)[68].

Impact on small and micro-businesses

370. It is expected that there would be very little impact on small and micro-businesses (SMBs), since all possible legitimate uses of SIM farms by SMBs have been exempted.

371. It is possible that not all customers of UK based suppliers and distributors will fall under the proposed exemptions. If this is the case, it is possible that some of these customers are SMBs and may see their revenue fall as they cannot obtain the devices.

[68] Nature of fraud and computer misuse in England and Wales - Office for National Statistics (ons.gov.uk): https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/natureoffraudandcomputermisuseinenglandandwales/yearendingmarch2022

372. The Home Office has conducted an extensive engagement process with legitimate suppliers of these devices and has not found any evidence of this to be the case.

Proportionality

373. There are a number of significant uncertainties in this analysis, and a number of assumptions have been made based on limited evidence. The best available data is used in the analysis, informed by experience and expertise.

374. The consultation included a call for evidence, which was designed to develop the evidence base and understanding of impacts going forwards.

375. No evidence from the call for evidence on scale of illegitimate use or harm caused was found.

376. External sector roundtables have been undertaken alongside the responses in the consultation to capture legitimate user issues. These have allowed the Government to better understand the sectors which may be impacted and how the policy will be practically implemented at a business level.

Risks and unintended consequences

377. 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. From extensive engagement with legitimate suppliers this risk is expected to be low.

    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.

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

379. 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.

380. The proposed legislation includes a provision that allows the Secretary of State to ban further technologies, to mitigate the risk around displacement.

381. The key analytical risk lies in lack of monetised analysis. Limitations in data and evidence meant this was not possible. However, evidence shows that the scale of the problem, and therefore potential benefits are high:

    - According to the August 2022 'Ofcom Scams Survey, in the period June-August 2022[69], an estimated 40.8 million adults in the UK reported they had received a suspicious message.
    - Of these people, an estimated 700,000[70] followed the scammer's instructions risking victimisation.
    - One police investigation discovered that five SIMs had sent over 900,000 messages in one SIM farm between April and October in one year.

[69] Ofcom Scams Survey, August 2022:
Ofcom CLI and scams research, August 2022 data tables

[70] Ofcom Scams Survey, August 2022:
Ofcom CLI and scams research, August 2022 data tables

382. This analytical risk is somewhat mitigated by the fact that the magnitude of expected potential benefits show that costs must be significantly higher than expected for VfM to be negative.

383. The goal of the policy is to frustrate criminals' abilities to send mass fraudulent calls and texts, through limiting their ability to access SIM farms, rather than stopping the problem completely.

Direct costs and benefits to business calculations

384. No direct costs to business have been monetised. The consultation included a call for evidence to collect information and data on the potential impacts of the SIM Farm ban. Due to the limited amount of evidence received, there remains uncertainties in relation to the impact of the proposal on businesses and the costs associated with introducing and implementing the ban[71]. Other than the cost of familiarisation with the guidance, the appraisal section therefore presents the non-monetised impacts on businesses from the proposed option.

Trade Impact

385. There may be a small negative trade impact because of the proposed change in legislation which would increase the burden on companies who legitimately import devices into the UK. Companies will be required to evidence they are importing the devices "in the course of business".

Wider impacts

386. It is not expected that there will be any wider environmental impacts as a result of this policy.

387. The proposed legislation allows the extension of the ban to other technologies that are at significant risk of being exploited by criminals to scam the public. The Secretary of State is able to specify further technologies via secondary legislation subject to the affirmative procedure in Parliament if certain criteria is met. This aims to ensure the government can act quickly if criminals start to use different methods of communications to send out scam texts or calls, to prevent displacement to other technologies.

[71] Preventing the use of SIM farms for fraud: government response (accessible): https://assets.publishing.service.gov.uk/media/655f3b45dcc6be000d5d1134/Government_Response_to_the_Consultation__Preventing_the_use_of_SIM_farms_for_fraud_.pdf

Annexes

Proposal 1: Reform the Identification Doctrine

Mandatory specific impact test - Statutory Equalities Duties	Complete
Under the current common law model, the identification doctrine disproportionately applies in practice to smaller business as it is easier to identify a person as their "directing mind and will". The burden is therefore currently proportionately higher in businesses with a lower headcount and centralised management structures. The extension to senior management aims to better capture and prosecute larger businesses compared to medium and smaller sized business. Senior managers are also more likely to be impacted by the measure. However, it is justified on the following basis: 1. The senior manager must commit a criminal offence to attribute liability to the company; 2. Senior managers take important decisions regarding the corporate policy and strategy of the company. This includes taking responsibility for how the business is managed and conducted, including delegating and supervising responsibilities to other employees. **The SRO has agreed these summary findings.**	**Yes**

Proposal 2: Suspension of Internet Protocol Addresses and Internet Domain Names

Mandatory specific impact test - Statutory Equalities Duties	Complete
There is limited evidence available to consider when having due regard for public-sector equality in relation to the provision. The Home Office publicly consulted on the Computer Misuse Act review in 2023, which included seeking views on suspending IP addresses and domain names, responses received were primarily from businesses, with some responses from individuals in the IT profession. Subsequent engagement with industry and law enforcement has not revealed any evidence of impacts that the proposed measures could have on persons with protected characteristics. We believe that the measure will not have a discriminatory effect against persons with any of the protected characteristics. Individuals may experience a positive impact from the measure due to the reduction in serious crime. **The SRO has agreed these summary findings.**	**Yes**

Proposal 3: Ban the supply or possession of devices known as 'SIM farms' in the UK

Mandatory specific impact test - Statutory Equalities Duties	**Complete**
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. There is no evidence as to who criminals are and as such it is not possible to assess impact. However, consultation responses would indicate the scale of use to be low, and as such it is highly unlikely the ban will have a disproportionate impact on any protected characteristics. The Home Office are aware that criminals often exploit vulnerable people and either trick or coerce them into committing a crime. However, there is no evidence that the risk of exploitation for this offence is or will be higher than in other crimes (for example, county lines) and LE already have systems in place to deal with such cases. Overall, the Home Office believe the benefits of these policies outweigh the 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 policy will effectively add barriers for fraudsters trying to contact potential victims, thus increasing protection for all potential victims, with or without protective characteristics. **The SRO has agreed these summary findings.**	**Yes**