

TOOLKIT

July 2026

Authorised Payment Fraud: Approaches to Policy and Governance

Georgia Jones, Olivier Kraft and Poornima Subramaniam

RUSI

Disclaimer

The content in this publication is provided for general information only. It is not intended to amount to advice on which you should rely. You must obtain professional or specialist advice before taking, or refraining from, any action based on the content in this publication.

The views expressed in this publication are those of the authors, and do not necessarily reflect the views of RUSI or any other institution.

To the fullest extent permitted by law, RUSI shall not be liable for any loss or damage of any nature whether foreseeable or unforeseeable (including, without limitation, in defamation) arising from or in connection with the reproduction, reliance on or use of the publication or any of the information contained in the publication by you or any third party. References to RUSI include its directors, trustees and employees.

© 2026 The Royal United Services Institute for Defence and Security Studies

This work is licensed under a Creative Commons Attribution – Non-Commercial – No-Derivatives 4.0 International Licence. For more information, see <http://creativecommons.org/licenses/by-nc-nd/4.0/>.

RUSI Research Papers, July 2026

ISSN 2977-960X

Publications Team

Editorial

Director of Publications: Alice Trouncer

Managing Editor: Sarah Hudson

Assistant Editor: Sophie Boulter

Assistant Editor: Liz Ottosson

Design

Graphic Designer: Lisa Westthorp

Research Editorial

Head of Research Governance and Editorial: Elias Forneris

Cover image: Courtesy of ภัทรชัย รัตนชัยวงค์ / Adobe Stock

Get in touch

www.rusi.org

enquiries@rusi.org

+44 (0)207 747 2600

The Royal United Services Institute for Defence and Security

61 Whitehall, London

SW1A 2ET

United Kingdom

Follow us on

Contents

2 Limitations

3 How to Use This Guide

5 Executive Summary

6 Introduction
6 Background and Scope
9 The Global Response

11 System-Level Design
12 Key Policy Design Considerations
23 Enablers for Effective Implementation and Operation

40 Intervention Design
40 Scope and Taxonomy
41 Intervention Characteristics

58 Conclusion

59 About the Authors

60 Annex 1: Interventions by Component and Primary Function

61 Annex 2: Navigating This Guide

63 Endnotes

© Royal United Services Institute

Methodology

Research for this paper was conducted from November 2025 to March 2026 with funding from the Gates Foundation. The research was conducted independently and all findings are the authors'. The paper was submitted on 26 May 2026 and approved for copy-editing on 16 June 2026.

Methodologically, this report is based on a comprehensive literature review, supplemented by semi-structured interviews held online with 36 stakeholders in 13 countries across public and private sectors and civil society.[1] Interviews were conducted on a non-attributable basis to ensure participants felt comfortable discussing sensitive operational and policy matters. Where conversations are cited, they are listed as 'Author interview', with the date and mode of conversation only.

An Advisory Board composed of five experts working in five different continents met three times over the course of the research to provide strategic direction.[2] Additionally, a series of validation conversations were held with subject-matter experts between 16 March 2026 and 31 March 2026. To identify relevant literature, a pre-existing repository of literature compiled for a project on a similar theme was consulted. In addition, relevant search strings were developed and run over both EBSCO and Google Scholar. The top results were reviewed, and those deemed relevant were examined in further detail. The findings of the literature review were then supplemented and validated through a series of interviews and consultations with experts.

The authors used Claude models Opus 4.6 and Sonnet 4.6 to assist with template design, drafting graphics, identification of additional sources and basic copy-editing.

1. Interviewees were in Armenia, Australia, Ghana, Indonesia, Kazakhstan, Malaysia, Mexico, Nigeria, the Philippines, South Africa and Turkey.
2. The advisory board was staffed with members from Australia, Malawi, the UK, the US and Vietnam.

© Royal United Services Institute

Limitations

The scope of this guide is limited in several ways.

- It does not examine unauthorised payment fraud, nor does it analyse policy responses from the perspective of adjacent criminal domains such as organised crime, human trafficking, cybercrime or terrorism financing.
- The guide does not substantively engage with the international dimensions of an effective anti-fraud response. While international cooperation is essential, effective cross-border collaboration depends on each country first having a sufficient domestic framework in place. Relevant resources on international initiatives and standards are referenced where applicable.
- The research underpinning this guide drew on sources in English, French and Spanish, which inevitably excludes insights from regions where policy has been shaped in other linguistic contexts.
- The guide does not provide a typology of the many manifestations of authorised payment fraud, as this ground is well covered by existing literature, including work by the UN Development Programme (UNDP) and the United Nations Office on Drugs and Crime (UNODC).
- While resource considerations are central to implementation, the authors do not attempt to break these down. The cost of interventions varies enormously depending on a country's starting point, institutional capacity, infrastructure and geography. The guide therefore identifies core components (many of which carry significant resource implications) while leaving questions of funding to be determined at the national level.
- The approach set out in this guide presupposes national authorities are willing to act. Where political will is entirely absent, the utility of its findings will naturally be limited.
- While underlining the importance of measuring effectiveness, the guide does not attempt to adjudicate the effectiveness of individual interventions, not least as 'success' is often contingent on a multiplicity of underlying enabling factors which vary greatly.
- Similarly, it is beyond the scope of this guide to discuss responses to broader policy issues, such as corruption and poverty, although these shape the effectiveness of anti-fraud measures.

© Royal United Services Institute

How to Use This Guide

This guide is designed as a practical resource for a range of readers working on authorised payment fraud, including policymakers, financial sector regulators, central banks, law enforcement and criminal justice officials, telecommunications and digital platform regulators, consumer and data protection authorities, and private sector practitioners in banks, payment providers, telecommunications companies (telcos) and platforms. Civil society organisations and researchers engaging with anti-fraud policy will also find relevant material throughout.

The guide can be read end-to-end or used as a reference tool. The following diagram breaks down the guide's contents by common priorities and signposts relevant sections as a starting point. Annex 2 contains a further breakdown of common queries raised and maps the guide's contents to these considerations.

© Royal United Services Institute



If you want to...

Get started / Build on your existing response

The five policy design considerations in Chapter I can be used as a diagnostic framework to identify what is already in place, what is partially developed, and where gaps remain.

The 15 intervention cards in Chapter II outline the prerequisites and dependencies for each intervention type, which can help determine how much existing infrastructure and legal frameworks support anti-fraud initiatives.

In addition to providing policymakers with a means to assess their own fraud landscape, clarify policy objectives and identify feasible interventions, this guide equips readers with a structured understanding of how fraud responses are practically designed and implemented. As such, it enables more effective engagement with the wider body of literature on anti-fraud policy, and a clearer basis on which to assess its potential relevance to their own jurisdiction.



Determine how to best prioritise a response in the context of limited resources

Chapter I provides guidance on how to determine the fraud types, sectors and payment channels jurisdictions can first prioritise, based on where risks are highest and entry points are clearest.

Each intervention card in Chapter II outlines a given initiative's dependencies and links with other interventions, which can help assess the feasibility of implementation. Prioritise interventions where the legal and operational prerequisites are already met or nearly so in a given jurisdiction. Interventions 7 and 13 have the fewest prerequisites and may be natural starting points for jurisdictions with constrained resources.



Identify the key actors to mobilise to combat authorised push payment (APP) fraud in a given jurisdiction

Chapter I outlines how to map delivery partners across the fraud lifecycle, based on who holds relevant data and has the capability to act, and discusses how to engage them early in the policy process.

The intervention cards in Chapter II outline the stakeholders critical to a given intervention's implementation.



Get buy-in to mobilise against authorised payment fraud

Chapter I discusses how fraud policy objectives can be anchored to broader national priorities, such as financial inclusion, digitalisation and public safety, to garner buy-in. It also provides guidance on how to assess the fraud landscape using existing data and targeted research methods, which can help build the evidence base needed to secure political will, funding and/or cross-departmental cooperation.

© Royal United Services Institute

Executive Summary

In response to rising levels of authorised payment fraud, a wave of international guidance and national strategies has emerged in recent years. Countries including Singapore, the UK and Australia have implemented national-level frameworks, while multilateral bodies such as the Financial Action Task Force (FATF), the UN and Interpol have released guidance and proposed standards which outline how jurisdictions can develop effective responses.

The available literature provides a rich evidence base to draw on. However, for policymakers in jurisdictions where a response is nascent, incorporating its insights in a way which makes sense in their own contexts can represent a practical challenge. Existing international guidance rightly focuses on establishing broad principles and standards, while national-level frameworks naturally reflect the specific contexts in which they were developed. This guide bridges that gap by offering an approach to understanding anti-fraud policy at a systems level and a means to help prioritise interventions in a way which reflects each jurisdiction's pre-existing conditions and constraints. It proposes a series of key design considerations and contextual factors which policymakers can employ to assess their own starting point and tailor a response for their respective jurisdiction. It profiles 15 widely adopted anti-fraud interventions, breaking them down by their key design characteristics to allow policymakers to assess which initiatives may be the most feasible and likely to have the most impact in their own jurisdiction.

© Royal United Services Institute

Introduction

Background and Scope

This guide focuses specifically on authorised payment fraud, often referred to as APP fraud,[3] or more colloquially known as a 'scam'. The guide uses the terms 'fraud' and 'scam' interchangeably.[4] The primary focus is to help policymakers in jurisdictions where a national-level response is nascent to develop effective policies and interventions which can be tailored to their context. Leveraging insights from a comprehensive literature review and interviews with 36 stakeholders in 13 countries, the guide identifies the key components common to a series of anti-fraud responses from across the world, paying particular attention to the factors which have contributed to their successful operationalisation.

Instead of prescribing a fixed set of measures, the guide offers policymakers a means to assess their own start point, develop their own objectives and consider which interventions may be most viable, have the most impact and be appropriately sequenced in their respective context.

Fraud is not only an issue of consumer protection or financial regulation, but a full-fledged security threat with far-reaching implications for institutional trust, economic stability and the integrity of the global financial system.[5] In recent years, the levels of authorised payment fraud,[6] whereby criminals mislead or coerce targets into initiating or approving payments, have been increasing.[7] The number of all fraud-related Interpol Notices and

3. Payment Systems Regulator, 'APP Scams', <https://www.psr.org.uk/our-work/app-scams/>, accessed 7 May 2026.
4. The authors acknowledge the critique that synonymous use of these terms can trivialise the offence and echo perpetrator framing. See Elisabeth Carter, Jack Mark Whittaker and Tim Day, 'More Than Splitting Hairs: Exploring Trivialisation and Harmful Narrative Distortion in the Synonymous Use of "Scam" and "Fraud"', *Crime, Media, Culture: An International Journal*, 23 November 2025, <https://doi.org/10.1177/17416590251393960>, accessed 12 June 2026. This paper retains both terms, as 'scam' is the operative term in many formal policy instruments globally.
5. Helena Wood et al., 'The Silent Threat: The Impact of Fraud on UK National Security', *RUSI Occasional Papers* (January 2021), <https://www.rusi.org/explore-our-research/publications/occasional-papers/silent-threat-impact-fraud-uk-national-security>, accessed 12 June 2026.
6. By contrast, unauthorised payment fraud occurs when criminals steal credentials or exploit compromised systems to initiate transactions without their target's knowledge.
7. Kathryn Westmore and Alison Owen, 'Following the Fraud: The Role of Money Mules', RUSI Emerging Insights, July 2025, <https://www.rusi.org/explore-our-research/publications/emerging-insights/following-fraud-role-money-mules>, accessed 12 June 2026.

© Royal United Services Institute

Diffusions has risen by 54% globally since 2024, and almost half of the world's population is estimated to be targeted by a scammer each week.[8] Meanwhile, scam operations have become increasingly 'polycriminal' enterprises, spilling into organised criminality, corruption, human trafficking, cybercrime and even terrorism.[9]

Citizens in developed countries may experience the highest average losses in absolute terms, but the financial impact in low- and middle-income countries (LMICs) is often far more pronounced relative to individual income and national economic output.[10] For instance, the Global Anti-Scams Alliance (GASA) estimates citizens in developing countries are more likely to lose money to a scam, and that these nations see a larger share of their GDP lost to scams.[11] Moreover, the UNDP notes the risk posed by scam operations is especially heightened in contexts where there are high levels of economic informality, low institutional capacity and pre-existing criminal groups – meaning many developing countries possess the characteristics which leave them particularly exposed to the propagation of illicit operations within their borders.[12]

The UNDP also highlights how the widespread use of digital platforms serves as another key vulnerability for fraud in LMICs.[13] Globally, internet penetration has increased dramatically, from about 16% of the population in 2005 to an estimated 74% in 2025.[14] LMICs in particular have seen extraordinary levels of growth in digital and mobile banking, encouraged by multilateral institutions such as the World Bank and the UN; indeed, Africa has been widely regarded as a global leader in digital and mobile banking.[15] However, while such innovations have improved levels of financial inclusion, they have also inadvertently opened up new populations to fraudsters, who now enjoy a steady supply of would-be targets in environments with insufficient oversight.[16]

8. Interpol, 'Global Financial Fraud Threat Assessment: Second Edition', press release, 16 March 2026, <https://www.interpol.int/en/News-and-Events/News/2026/INTERPOL-report-warns-of-increasingly-sophisticated-global-financial-fraud-threat>, accessed 12 June 2026; Global Anti-Scam Alliance (GASA) and Feedzai, 'Global State of Scams 2025 Report', 7 October 2025, <https://www.gasa.org/post/global-scams-on-the-rise-over-half-of-adults-worldwide-report-scam-encounters>, accessed 12 June 2026.
9. Interpol, 'Global Financial Fraud Threat Assessment'.
10. GASA and Feedzai, 'Global State of Scams 2025 Report', p. 16.
11. *Ibid.*, pp. 15, 17.
12. Joe Hooper, Bill Bannear and Gary Chew, 'Anti-Scam Handbook v2.0: Collective Response and Tools to Safeguard Development', Section 2.0, UN Development Programme (UNDP), 2025, <https://www.undp.org/policy-centre/singapore/publications/anti-scam-handbook>, accessed 12 June 2026.
13. *Ibid.*
14. World Bank Group, 'Individuals Using the Internet (% of Population), 1990–2025', <https://data.worldbank.org/indicator/IT.NET.USER.ZS>, accessed 12 June 2026.
15. GSMA, 'State of the Industry Report on Mobile Money 2026', 2026, <https://www.gsma.com/sotir/>, accessed 12 June 2026; World Economic Forum, 'Here's Why Africa is the World Leader in Digital and Mobile Banking', 21 November 2023, <https://www.weforum.org/stories/geographies-in-depth/africa-digital-mobile-banking-financial-inclusion/>, accessed 12 June 2026.
16. Through the lens of Routine Activity Theory, the rise in scams can be understood as a product of three factors: motivated offenders, a steady supply of targets and insufficient oversight. See Lawrence E Cohen and Marcus Felson, 'Social Change and Crime Rate Trends: A Routine Activity Approach', *American Sociological Review* (Vol. 44, No. 4, August 1979), pp. 588–608.

© Royal United Services Institute

The world over, policymakers have been left scrambling to combat the historic increase in scams, which resulted in an estimated $442 billion lost in 2025 alone, generating profits that some commentators assert rival those of the illicit drugs trade.[17] LMICs, however, have been left especially exposed following unprecedented declines in the levels of official development assistance (ODA), which have greatly narrowed the capital available to governments in these countries to fund a response.[18]

While reductions in ODA have left many LMIC governments struggling across multiple policy domains, failure to meaningfully stem the tide of scams risks imposing harmful long-term impacts on trust and economic stability. Moreover, failure to adequately address consumer concerns around fraud risks reversing an entire generation of financial inclusion gains, should more victims lose trust in the formal financial sector.[19] Were more people in LMICs to elect to 'self-exclude' from engaging with the formal economy due to reduced trust, this would, as FATF has clearly stated, increase the risk of money laundering (ML) and/or terrorist financing (TF) in these countries.[20] Ensuring fraud is properly dealt with, therefore, is a precondition for a well-functioning anti-money laundering / countering the financing of terrorism (AML/CFT) regime.

It is not, however, solely in the interest of LMICs to safeguard against the deleterious effects of widespread scams. Authorised payment fraud is often transnational in nature, meaning the vulnerability of developing countries should be of huge concern for developed countries too. In the UK, for example, an estimated two-thirds of fraudulent schemes targeting the British public originate overseas.[21] As such, ensuring all countries are equipped to respond effectively on a domestic level will prove essential in tackling this growing global threat.

17. GASA and Feedzai, 'Global State of Scams 2025 Report'; *The Economist*, 'Online Scams May Already be as Big a Scourge as Illegal Drugs', 6 February 2025.
18. Organisation for Economic Co-operation and Development (OECD), 'A Historic Decline in Foreign Aid: Preliminary 2025 ODA Data', 9 April 2026, <https://www.oecd.org/en/data/insights/data-explainers/2026/04/a-historic-decline-in-foreign-aid-preliminary-2025-oda-data.html>, accessed 12 June 2026.
19. Eric Duflos, 'Findex 2025: Why Financial Inclusion Needs to be More Responsible', blog, 29 August 2025, <https://www.cgap.org/blog/findex-2025-why-financial-inclusion-needs-to-be-more-responsible>, accessed 12 June 2026.
20. Financial Action Task Force (FATF), 'FATF Guidance: Financial Inclusion and Anti-Money Laundering and Terrorist Financing Measures', June 2025, <https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-Financial-Inclusion%20-Anti-Money-Laundering-Terrorist-Financing-Measures.pdf.coredownload.pdf>, accessed 12 June 2026.
21. Home Office, 'Global Taskforce Launched to Hunt Down Overseas Scammers', press release, 17 March 2026, <https://www.gov.uk/government/news/global-taskforce-launched-to-hunt-down-overseas-scammers>, accessed 12 June 2026.

© Royal United Services Institute

The Global Response

In response to growing levels of APP fraud, actors across the private, national and multilateral levels have endorsed a wave of policies aimed at strengthening prevention and prosecution. Modern fraud campaigns are most often implemented across multiple platforms and are enabled in large part by fragmented oversight, resulting in isolated, single-sector interventions which are unlikely to be sufficient in meaningfully stemming the tide of scams. As such, despite differences in detail, the extant anti-fraud policies and guidance reviewed for this guide converge around a broadly consistent vision of what an effective domestic response looks like: one which engages stakeholders from across the public and private sectors, distributes legal obligations appropriately, fosters cross-sectoral collaboration, sets well-defined objectives and establishes clear leadership and accountability.

Several developed countries which have experienced high levels of fraud losses have implemented national-level strategies embodying exactly these qualities. Singapore, for example, established one of the world's first anti-scam centres in 2019.[22] It also adopted its Shared Responsibility Framework in 2024, placing obligations on the country's financial institutions and telcos to combat phishing scams.[23] The UK, meanwhile, updated its Fraud Strategy in 2026, setting out a whole-of-system approach to tackling what is the country's most prevalent crime, and announcing the creation of an Online Crime Centre which brings the public and private sectors together to fight fraud.[24] Australia, too, passed a Scams Prevention Framework (SPF) in 2025, which has effectively legislated a collective action response from across society, and established obligations for digital platforms, banks and telcos in the country's anti-scam efforts. [25]

In recent years, multilateral agencies have also released guidance with helpful insights for policymakers from a more jurisdictionally agnostic perspective explaining how to design a response which successfully rallies a whole-of-system response to fraud. The UNDP's Anti-Scam Handbook provides a useful typology of digital scam types, along with a detailed map visualising the individual, institutional and systemic constituents policymakers should consider when examining fraud in their respective jurisdiction.[26] FATF also released two rounds of guidance in 2023 and 2026, sharing best practices for combatting digitally enabled fraud by better leveraging the existing components of AML/CFT frameworks to strengthen

22. Dominic Dass, 'The Anti-Scam Centre: A Collaborative Approach Against Scams', Signapore Police Force, 29 November 2021, <https://www.police.gov.sg/media-hub/police-life/2021/11/the-anti-scam-centre---a-collaborative-approach-against-scams>, accessed 12 June 2026.
23. Monetary Authority of Singapore, 'Guidelines on Shared Responsibility Framework', 24 October 2024, <https://www.mas.gov.sg/regulation/guidelines/guidelines-on-shared-responsibility-framework>, accessed 12 June 2026.
24. Home Office, 'New Disruption Unit Launched in Crackdown on Fraud', press release, 9 March 2026, <https://www.gov.uk/government/news/new-disruption-unit-launched-in-crackdown-on-fraud>, accessed 12 June 2026.
25. Department of the Treasury (Australia), 'Scams Prevention Framework: Protecting Australians from Scams', January 2025, <https://treasury.gov.au/publication/p2025-623966>, accessed 12 June 2026.
26. Hooper, Bannear and Chew, 'Anti-Scam Handbook v2.0'.

© Royal United Services Institute

public and private sector coordination to detect, disrupt and recover the proceeds of fraud.[27] In 2026, ASEAN shared a paper documenting best practices against scams perpetrated via SMS and calls, proposing a tiered framework for member states to work with their domestic telco sectors in a way which acknowledges respective technical capacity and risk profiles.[28] Interpol, too, outlined a series of recommendations to foster a better domestic response in its second Global Financial Fraud Threat Assessment, released in 2026, and produced confidential guidelines for law enforcement agencies looking to establish national anti-scam centres.[29]

The available literature provides a rich evidence base to draw on. However, for policymakers in jurisdictions where a response is nascent, incorporating its insights in a way which makes sense in their own contexts can represent a practical challenge. Existing international guidance rightly focuses on establishing broad principles and standards, while national-level frameworks naturally reflect the specific contexts in which they were developed.

The remainder of this guide is designed to help bridge this gap. Chapter I presents five key considerations for developing an effective systemic response to fraud, offering practical guidance on determining risk, setting objectives and identifying the actors needed to drive an anti-fraud agenda. It also highlights the broader ecosystem of laws, regulations and governance processes on which effective implementation depends. Chapter II profiles the 15 most common intervention types deployed against fraud. Each intervention card outlines core design considerations, describes what successful implementation requires, and points to relevant international standards, examples and further resources.

27. FATF, Egmont Group and Interpol, 'Illicit Financial Flows from Cyber-Enabled Fraud', 9 November 2023, <https://www.fatf-gafi.org/en/publications/Methodsandtrends/illicit-financial-flows-cyber-enabled-fraud.html>, accessed 12 June 2026; FATF, 'Cyber-Enabled Fraud: Digitalisation and Money Laundering, Terrorist Financing and Proliferation Financing Risks', 24 February 2026, <https://www.fatf-gafi.org/en/publications/Methodsandtrends/cyber-enabled-fraud-digitalisation-ml-tf-pf-risks.html>, accessed 12 June 2026.
28. ASEAN, 'ASEAN Guide on Anti-Scam Policies and Best Practices', January 2026, <https://asean.org/wp-content/uploads/2026/01/ASEAN-Guide-on-Anti-Scam-Policies-and-Best-Practices-090126.pdf>, accessed 12 June 2026.
29. Interpol, 'Global Financial Fraud Threat Assessment'.

© Royal United Services Institute

System-Level Design

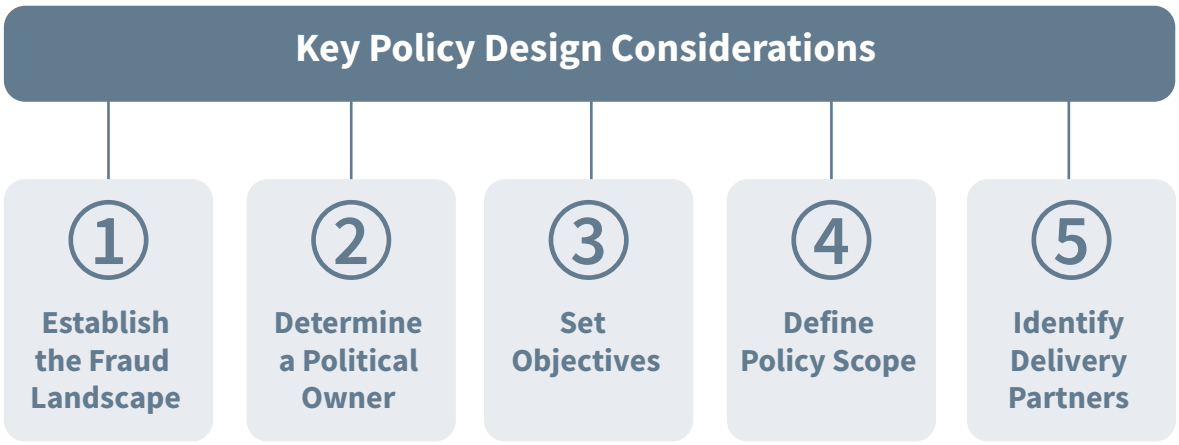
Fraud responses globally have typically evolved in response to an immediate problem. Most often, interventions have evolved locally within a specific sector or channel which then drives full system integration and increased participation. Lessons drawn from country experiences, expert consultations and broader literature suggest implementing interventions without foundational policy-level decisions results in downstream challenges including problems with measuring effectiveness, or limited information-sharing, reach or participation. This chapter therefore recommends system-level thinking as a deliberate starting point, even where a country is only in a position to implement one or a few initial interventions, to ensure they are guided by broader objectives which can be scaled or adjusted over time. Subsequently, the interventions profiled in Chapter II contain examples of cross-dependencies to help inform incremental implementation.

First, this chapter draws on literature and the experience of researched countries to propose five policy design considerations that are common denominators for designing a fraud response framework. Second, it highlights governance processes and requirements which enable the system architecture to be operationalised effectively. Both sections provide practical considerations and examples from international practice. Because there is no single 'correct' model, any examples provided illustrate possible pathways rather than defining a prescriptive or exhaustive set of choices. Similarly, the order in which policymakers address the considerations outlined below will depend entirely on their context: in some jurisdictions establishing a political owner may need to come before any further actions can be taken, whereas in others establishing a clear picture of the fraud landscape may make more sense as a first step.

© Royal United Services Institute

Key Policy Design Considerations

Figure 1: Key Entry Points for Policy Design



Source: The authors.

Consideration 1: Establish the Fraud Landscape

An effective anti-fraud policy should begin by understanding the existing fraud landscape. Policymakers should know what kinds of scams exist, how widespread they are, who is affected, and which institutions are already trying to prevent or respond to scams. This assessment provides the baseline for setting policy priorities, defining clear objectives and determining which agencies and sectors need to be involved.

Analysing the existing sources of information showing the scale, nature and impact of fraud can significantly help policymakers understand the threats and vulnerabilities in their respective jurisdiction. Data may already be available in existing ML/TF National Risk Assessments (NRAs) or can be scattered across different authorities and sectors. For example, victimisation surveys, consumer complaints submitted to consumer protection agencies, fraud papers collected by banks and payment providers, data held by telecommunications regulators, and law enforcement case records can all reveal information about scam prevalence and affected groups. Additionally, civil society organisations and consumer rights groups may also hold data which can help to provide a clearer analysis of the threats and vulnerabilities present. Countries may also be able to rely on private or civil sector surveys on regional- or country-level scams. For example, GASA conducts global surveys of scams providing regional breakdowns as part of its annual 'State of Scams' consumer survey papers.[30]

30. GASA, 'GASA Knowledge Base', <https://gasa.org/knowledge-base?content_group=318467252980&page=1>, accessed 12 June 2026.

© Royal United Services Institute

Where formal guiding systems or administrative data are limited, countries can supplement their understanding through targeted research. The following are some examples of such approaches:

- **Victimisation surveys**: Adding fraud as a category to existing national victimisation surveys can be a low-cost way to establish the prevalence and demographic exposure to fraud in a given jurisdiction. The UK's Crime Survey for England and Wales has incorporated fraud and computer misuse since 2017, and the resulting data is now central to the country's anti-fraud strategy and resourcing decisions.[31] Similarly, many countries in Latin America and the Caribbean which conduct victimisation surveys to understand insecurity have embedded fraud as a category within their analysis.[32]
- **Consumer surveys**: The Consultative Group to Assist the Poor (CGAP) recommends the use of surveys to establish understanding of consumer risk.[33]
- **Workshops, advisory panels and focus groups**: These can rapidly generate insights where large-scale data collection is not feasible. Bringing together law enforcement agencies, consumer protection authorities, financial institutions, telcos and civil society organisations can create evidence and provide a map of ongoing prevention and response initiatives. For example, a multistakeholder workshop held in Cambodia in 2024, co-organised by national ministries and the UNDP, gathered 40 experts from 20 organisations to assess the impact of digital scams, review ongoing anti-fraud efforts and identify areas for improved coordination.[34]

31. Office for National Statistics, 'Crime in England and Wales: Year Ending December 2025', 23 April 2026, <https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/latest>, accessed 12 June 2026.
32. United Nations Office on Drugs and Crime (UNODC), 'Victimization Surveys in Latin America: Reliable Data to Strengthen Peace, Justice and Public Trust', 22 October 2025, <https://www.cdeunodc.inegi.org.mx/unodc/index.php/2025/10/22/victimization-surveys-in-latin-america-reliable-data-to-strengthen-peace-justice-and-public-trust/index.htm>, accessed 12 June 2026.
33. Author interview, online, 19 February 2026.
34. Hooper, Banner and Chew, 'Anti-Scam Handbook, v2.0', p. 71.

© Royal United Services Institute

RESOURCES **01**

Further Guidance and Tools to Assess the Fraud Landscape



- **CGAP**: Consumer survey template on the risks associated with the use of digital financial services, designed for financial authorities[35]
- **UNODC**: Manual on Victimisation Surveys[36]
- **World Bank**: Free survey design solution[37]

Consideration 2: Determine a Political Owner

In addition to conducting analysis of the fraud and policy landscape, policymakers looking to develop a coordinated response to fraud should consider the key stakeholders they will need to drive impact. Clear political ownership is essential to encourage the collective action needed for effective anti-scam responses across consumers, the private sector and public agencies. Interviews with experts reveal that a lack of political ownership can have an impact on the pace of action (for example, through resourcing and priority-setting)[38] and efficacy of cooperation (for example, through legal reform and ensuring cooperation across departments).[39]

Senior political ownership can help anti-fraud policy in three main ways. First, it signals tackling fraud as a national priority. Second, it builds legitimacy for tough decisions (such as funding), helps galvanise resource allocation both in public agencies and in private companies, and resolves competing priorities between different actors. Third, it can drive, through visible championing, necessary behaviour changes among institutions, industry and consumers.

Key factors for effective political ownership include political seniority, strong convening powers[40] and political reach to visibly champion consumer behaviour change. Determining political ownership is, thus, country specific. Some international approaches to political ownership include:

- **Named minister**: A designated fraud minister is appointed with statutory powers, giving the fraud agenda cabinet-level significance (for example, in the UK).

35. CGAP, 'Survey on the Risks Associated with the Use of Digital Financial Services, Designed for Financial Authorities', September 2023, <https://www.cgap.org/sites/default/files/2023-09/Survey-Questionnaire-on-DFS-Consumer-Risks.pdf>, accessed 12 June 2026.
36. UNODC, 'Manual on Victimisation Surveys', 2009, <https://www.unodc.org/documents/data-and-analysis/Crime-statistics/Manual_on_Victimization_surveys_2009_web.pdf>, accessed 12 June 2026.
37. World Bank, 'Survey Solutions', <https://mysurvey.solutions/en/>, accessed 12 June 2026.
38. Author interview, online, 17 February 2026.
39. Author interviews, online, 28 January 2026 and 17 February 2026.
40. Author interview, online, 26 January 2026.

© Royal United Services Institute

- **President / prime minister**: The president or prime minister visibly drives and champions the fraud policy (for example, in Cambodia,[41] Indonesia,[42] Korea,[43] Thailand[44] and Taiwan[45]).
- **Ministerial ownership**: A ministry or department owns the fraud agenda with the respective minister or head of the department driving it. Examples include the Ministry of Home Affairs in Singapore[46], Ministry of Digital Economy and Communications in New Zealand[47], and the Attorney-General in Australia[48].

Several countries have implemented interventions, with varying degrees of success, without dedicated political ownership, relying instead on central bank leadership (for example, in Armenia,[49] Egypt,[50] Ghana[51] and the Philippines[52]) or distributed arrangements (for example, in Mexico[53]). These approaches have proven to be successful start points where central banks wield significant authority and the anti-fraud focus is confined to the financial sector. However, this model may be structurally limited in delivering cross-sector momentum essential for systemic fraud response as central banks may have limited ability to align cross-sector priorities,[54] necessary regulatory reform and law enforcement measures, or deliver citizen-level victim support.

41. Sovann Sreypich, 'Phnom Penh Sets Up Anti-Scam Task Force Amid Rising Online Scams', *CamboJA News*, 4 July 2025, <https://cambojanews.com/phnom-penh-sets-up-anti-scam-task-force-amid-rising-online-scams/>, accessed 12 June 2026.
42. Author interview, online, 28 January 2026.
43. Lee Jung-joo, 'South Korean President Lee Orders Tougher Crackdown on Overseas Telecom Scams', Asia News Network, 22 October 2025, <https://asianews.network/south-korean-president-lee-orders-tougher-crackdown-on-overseas-telecom-scams/>, accessed 12 June 2026.
44. Author interview, online, 17 February 2026.
45. *Radio Taiwan International* (RTI), 'President Lai Details Taiwan's Anti-Fraud Policy Updates', 17 April 2025, <https://www.rti.org.tw/en/news?uid=3&pid=124625>, accessed 12 June 2026; Executive Yuan, R.O.C. (Taiwan), 'Premier Calls for Tough Action on Cross-Border Telecom Fraud', press release, 14 September 2017, <https://english.ey.gov.tw/Page/61BF20C3E89B856/ae0b37c2-cdff-428e-bf9c-2806d4d4702c>, accessed 12 June 2026.
46. Ministry of Home Affairs (Singapore), 'Written Reply to Parliamentary Question on the Agencies and Organisations that Have Partnered the Anti-Scam Command to Raise Awareness on Scams and Protect Singaporeans', 1 August 2022, <https://www.mha.gov.sg/media-room/newsroom/written-reply-to-pq-on-the-agencies-and-organisations-that-have-partnered-the-anti-scam-command-to-raise-awareness-on-scams-and-protect-singaporeans/>, accessed 12 June 2026.
47. Author interview, online, 26 January 2026.
48. Commonwealth Fraud Prevention Centre, Attorney-General's Department (Australia), 'Report Fraud', <https://www.counterfraud.gov.au/report-fraud>, accessed 23 March 2026.
49. Author interview, online, 4 December 2025.
50. Mostafa Khidr, 'From Detection to Disruption: Building a Central Bank-Led National Framework to Combat Fraud and Financial Crime', speech given at the UNODC Global Fraud Summit, Vienna, 2026.
51. Author interview, online, 25 November 2025.
52. Section 23 of the Anti-Financial Account Scamming Act empowers the Bangko Sentral ng Pilipinas in relation to implementing provisions of the Act, in coordination with other agencies including the Cybercrime Investigation and Coordination Center. See Anti-Financial Account Scamming Act, p. 12, <https://www.bsp.gov.ph/Regulations/Banking%20Laws/AFASA-Booklet-with-IRRs.pdf>, accessed 12 June 2026.
53. Author interview, online, 9 December 2025.
54. Author interview, online, 26 January 2026.

© Royal United Services Institute

EXAMPLES **01**

Political Ownership in Action

Thailand: The prime minister chairs the National Committee on Technology Crime, personally launched the 2025 United Citizens Against Scammers campaign, and announced a shift from defensive to offensive strategies. Such ownership has enabled participation of the financial sector and payment networks and collaboration between them and law enforcement agencies.[55]

UK: A dedicated fraud minister was appointed in 2024 who has overseen the launch of the UK's new fraud reporting portal and the 2026–2029 UK Fraud Strategy.[56]

Consideration 3: Set Objectives

For some contexts, reducing fraud losses may be the primary objective. For others, tackling fraud may be secondary to wider goals such as reducing / interrupting crime, expanding digital payments, promoting financial inclusion, or sustainable development. Setting out 'overarching objectives' provides direction for policy design and shows how it interacts with other national priorities.

More granularly, setting 'policy objectives' could inform which interventions should be prioritised, and the actors needed to deliver them. They also help translate the policy vision into measurable indicators and metrics, enabling periodic evaluation of policy effectiveness. Each policy objective may require different sets of metrics, with relevant delivery partners or governance bodies responsible for collecting the necessary data. Policymakers can then use this data to periodically assess whether the policy is achieving its intended objectives.

Setting Overarching Objectives: These broadly set out why the country is tackling fraud. This helps situate the fraud policy within the national agenda and mitigates siloed policymaking by creating a shared understanding of how combatting fraud is essential for the success of other national priorities such as digitisation and financial inclusion.

Policies introduce these at their outset. For example, Australia's 2025 Scam Prevention Framework has a half page titled 'Why is action needed?'.[57] Other examples of overarching objectives are provided in Table 1.

55. Author interview, online, 17 February 2026.
56. UK Government, *Fraud Strategy 2026–2029: Disrupting Crime, Supporting Economic Resilience and Delivering Justice*, CP 1523 (London: The Stationery Office, 2026).
57. Department of the Treasury (Australia), 'Scams Prevention Framework'.

© Royal United Services Institute

Setting Policy Objectives: This involves specifying goals and pathways for policy implementation. Derived from risk assessments, overarching objectives, fiscal constraints and political feasibility, these objectives shape actionable plans, performance indicators and intervention sequencing. Guidance issued by the European Anti-Fraud Office's objective-setting for Anti-Fraud Strategies for the EU recommends they should be 'Specific, Measurable, Achievable, Realistic/Relevant, and Time-bound (SMART)', and 'not too numerous to allow a proper and realistic implementation'.[58]

Existing policies typically have three main policy objectives (see Table 1): to punish crime; to support victim recovery; and to curtail the flow of harmful activity (prevention, detection and disruption). A UNODC fraud action plan checklist, sets out four objectives under 'Prevent', 'Pursue', 'Protect' and 'Promote' (for example, cooperation and shared goals).[59]

Objective-setting around victim harm may vary vastly across countries as there are many different harms caused by fraud aside from financial loss to victims. Victim harm can be physical in many countries, such as human trafficking or coercion.[60] Victim harms can also be psychological, impacting livelihoods as well as trust in financial systems or law enforcement. For countries prioritising victim harm reduction, Peru's National Multisector Policy against Organised Crime (2019–30) prioritises assistance to victims as among its main objectives. It highlights the role of capabilities, such as citizen participation, in countering organised crime and aiding affected persons, including through judicial protection of victims.[61]

58. European Anti-Fraud Office, European Commission, 'Guidelines on National Anti-Fraud Strategies', December 2016, p. 46, <https://sfc.ec.europa.eu/sites/default/files/EN-ORI-General%20Guidelines%20on%20National%20Anti-Fraud%20Strategies%20ARES%282016%296943965.pdf>, accessed 12 June 2026.
59. UNODC, 'Organized Fraud', issue paper, 2024, pp. 60-61, <https://www.unodc.org/documents/organized-crime/Publications/IssuePaperFraud-eBook.pdf>, accessed 12 June 2026.
60. As of March 2025, the UN estimated that victims from 66 countries were trafficked into online scam centres. See UN, 'UN Report Exposes Torture, Rape in Southeast Asia's Multi-Billion-Dollar Scam Centres', 20 February 2026, <https://news.un.org/en/story/2026/02/1167012>, accessed 12 June 2026.
61. UNODC, 'Organised Crime Strategy Toolkit for Developing High Impact Strategies', 2021, Case Study 7, p. 22, <https://www.unodc.org/cld/uploads/pdf/Strategies/OC_Strategy_Toolkit_Ebook.pdf>, accessed 12 June 2026.

© Royal United Services Institute

Table 1: Key Frameworks by Overarching / Policy Objectives

Framework / Policy Guidance	Overarching Objectives	Policy Objectives
Australia 2025 Scams Prevention Framework[62]	• trust in the digital economy • consumer protection • harm reduction	• prevent scams • detect scams • disrupt scams
Nigeria Draft Guidelines for Handling APP Fraud[63]	• protection of public trust • financial inclusion • financial system resilience • protection of the payment system	• prevent APP fraud • detect APP fraud • report APP fraud • resolve APP fraud
Saudi Arabia 2022 Saudi Central Bank Counter-Fraud Framework[64]	• economic stability • consumer protection • making the country unattractive for fraudsters	• prevent fraud • detect fraud • respond to fraud
Taiwan 2024 Next Generation Anti-Fraud Strategy Guidelines[65]	• reduction in harm • reduction in exposure • reduction in deception	• identify fraud • prevent fraud • intercept fraud • punish fraud
UK 2026–2029 Fraud Strategy[66]	• crime reduction • economic resilience • scaling of existing measures for effectiveness	• disrupt fraud • safeguard consumers • respond (support victims and deliver justice)

Consideration 4: Define Policy Scope

Balancing ambition with feasibility requires early scoping of the policy framework, by prioritising high-impact risks, ensuring alignment with objectives and considering national priorities. Scope, here, refers to the policy's boundaries: the types of fraud addressed, sectors involved, actors covered and payment types.

Defining the right scope is a balancing act between what addresses the defined objectives and what is technically, operationally, fiscally and legally feasible. If the scope is too narrow, it is highly likely the fraud risk will simply migrate. If the scope is too broad it

62. Department of the Treasury (Australia), 'Scams Prevention Framework'.
63. Guidelines of the Central Bank of Nigeria on APP fraud (in draft at time of writing): Central Bank of Nigeria, 'Exposure Draft of the Guidelines for Handling Authorised Push Payment Fraud' 26 November 2025, <https://www.cbn.gov.ng/Out/2025/CCD/Exposure%20draft%20of%20the%20Guidelines%20for%20Handling%20Authorised%20Push%20Payment%20Fraud.pdf>, accessed 12 June 2026.
64. Saudi Central Bank, 'Counter-Fraud Framework', 11 October 2022, <https://rulebook.sama.gov.sa/en/counter-fraud-framework-0>, accessed 3 July 2026.
65. Executive Yuan, 'Next-Generation Anti-Fraud Strategy Guidelines, Version 2.0', 6 December 2024, <https://english.ey.gov.tw/News3/9E5540D592A5FECD/faccc48c-1d4c-45c8-aa1b-73d9c283a73d>, accessed 3 July 2026.
66. UK Government, *Fraud Strategy 2026–2029*.

© Royal United Services Institute

will be operationally challenging and add governance and coordination burden to participants; a whole-of-economy approach involving multiple sectors requires more coordination, data-sharing and privacy considerations, a broader legal framework and broader set of common standards.

There are a number of practical considerations in determining what is manageable and what to start with. The following are examples based on the authors' research and demonstrate a range of approaches which have been taken internationally.

- **Focusing on greatest risk and points of control**: International practice shows jurisdictions typically prioritise fraud types and channels where the impacts of fraud are highest and intervention points are clearest. How this manifests in each jurisdiction will depend on the nature of the threat: in some countries the greatest risk may be skyrocketing fraud losses, in others it could be the human trafficking of citizens into scam compounds by organised criminals.
- **Starting where reporting structures currently exist**: Many countries have developed their response to authorised payment fraud by expanding existing regulatory oversight in financial, telecommunications and technology sectors. For example, the financial regulator of Kazakhstan's Astana International Financial Centre has established conduct expectations and reporting requirements related to fraud for all financial entities it regulates. This includes reporting on fraud, imposing internal control requirements using a risk-based approach for fraud, and ensuring consistent outcomes for consumers through consumer complaints-handling processes and consumer redress.[67]
- Other countries have added authorised payment fraud to the remit of existing cybercrime or fraud architectures. Turkey has expanded information-sharing and experience of the Interbank Card Centre to include all types of fraud.[68] Vietnam is building on the strengths of its existing cybercrime centre to play a national coordinating role for all types of scams.[69]
- **Expanding on AML/CFT Frameworks (also see Intervention 1):** In line with FATF guidance, many countries are currently tackling fraud by expanding existing interventions. Some countries, such as Ghana, Mexico,[70] Nigeria and Armenia[71] are leveraging their existing AML/CFT architecture to impose duties, such as due diligence, monitoring, reporting and cooperation, relating to fraud. The Nigerian Central Bank requires financial institutions to have dedicated fraud teams alongside their compliance teams.[72]

67. Author interview, online, 3 December 2025.
68. Author interview, online, 5 January 2026.
69. Author interview, online, 3 December 2025.
70. Author interview, online, 9 December 2025.
71. Author interview, online, 4 December 2025.
72. Author interview, online, 13 December 2025.

© Royal United Services Institute

Consideration 5: Identify Delivery Partners

Tackling fraud requires cooperation from multiple actors, including consumers. Research interviews with experts show that identifying who is required to deliver the policy in practice, and engaging them early on, benefits the policymaking process.[73] This can help set realistic definitions of roles and responsibilities, and ensure operational constraints are understood, incentives are aligned (further explained in Enabler 1.3 Incentives below) and buy-in is secured. For example, the UK's Fraud Strategy 2026–2029 outlines 'delivery partners' across four categories: departments and non-departmental public bodies; law enforcement and intelligence partners; private sector partners; and the public, civil society, and NGOs.[74]

There is no universal guidance on which partners should be involved, although generally marshalling support from across law enforcement, government, civil society, and public and private sectors is necessary to design an effective response. Determining the exact partners will depend on each country's fraud threat landscape, existing data infrastructure and policy objectives. In Malaysia, for example, where anti-fraud efforts are centred around the National Fraud Portal and supported by an extensive payment network, the identification of relevant actors has developed in relation to how fraud data is generated within the financial sector, shared with the portal, and subsequently acted upon.[75]

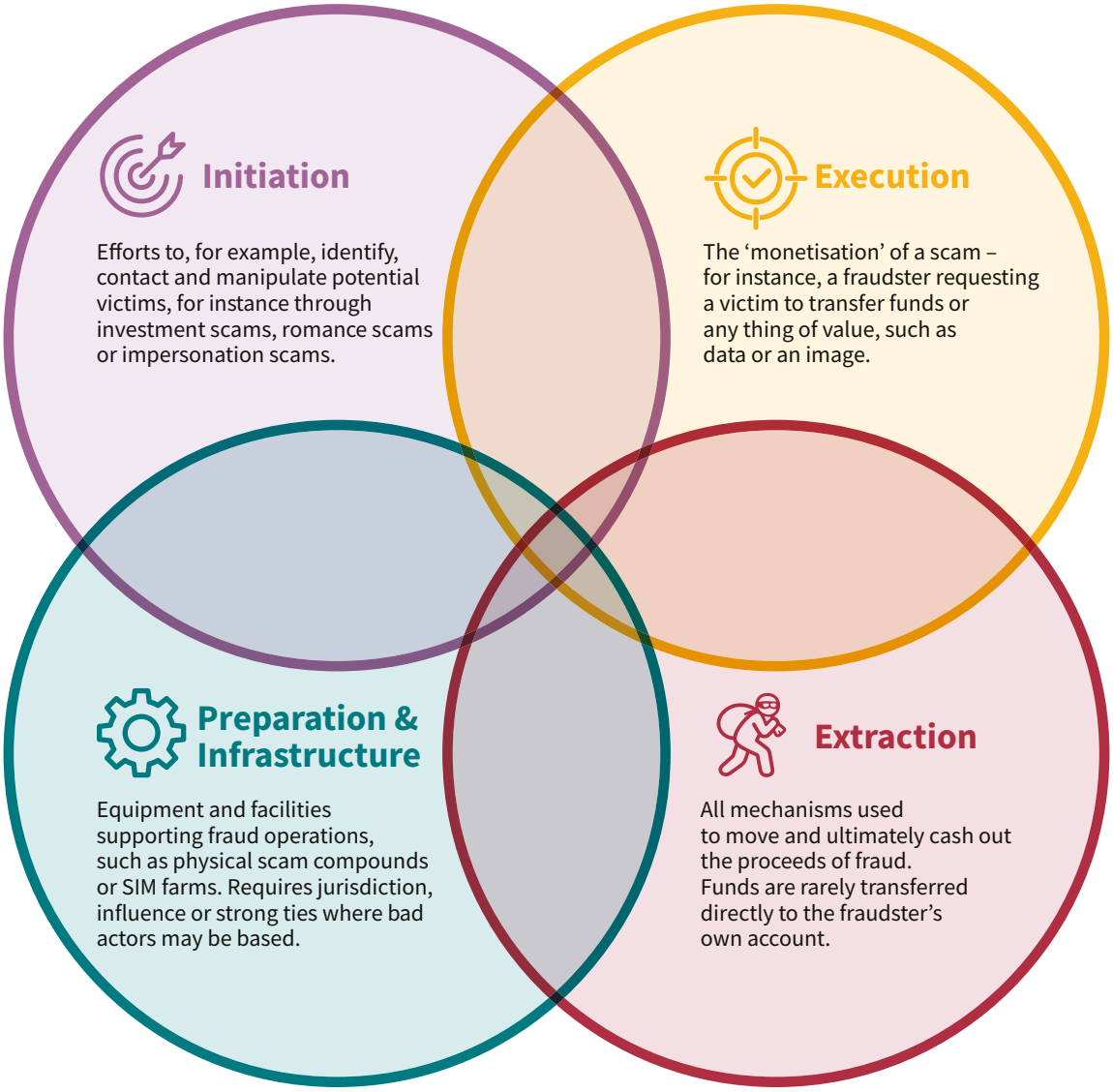
When mapping out potential stakeholders to deliver interventions, an assessment of the existing levels of trust based on an initiative's required partners and objectives would also be of great benefit, as determining the most effective partners may in large part depend on 'who trusts who' in a particular context. For example, a public awareness campaign may carry more weight coming from a central bank in one jurisdiction whereas in another a consumer protection body may be better placed to share the message.

In some contexts, policymakers draw on the methods of fraudsters[76] (often referred to as the 'fraud chain') as a way of identifying relevant actors required to disrupt them. This approach maps fraud as a set of components, such as initiation, preparation and infrastructure, execution, and extraction (see Figure 2) and considers which actors have a role within each component of the chain and what this role may be. The term 'component' is used rather than 'stage' to reflect they are neither linear nor sequential. In practice, different components may overlap and the line between them may not always be clear. To support policymakers in linking stakeholders to relevant points in the fraud system, each intervention in Chapter II is accompanied by markers indicating the component(s) to which it could relate.

73. Recommendations from the Advisory Board for the research study for this guide.
74. UK Government, *Fraud Strategy 2026–2029*.
75. Author interview, online, 13 January 2026.
76. Hooper, Banner and Chew, 'Anti-Scam Handbook, v2.0', p. 66.

© Royal United Services Institute

Figure 2: The Fraud Chain



Source: The authors, building on: Fraud Kill Chain Foundation, 'Fraud Kill Chain White Paper V2', April 2025, <https://www.fraudkillchain.com/wp-content/uploads/2025/04/Fraud-Kill-Chain-White-Paper-V2.pdf>, accessed 1 July 2026; and House of Lords Fraud Act 2006 and Digital Fraud Committee, 'Fighting Fraud: Breaking the Chain', 2022, p. 73, <https://committees.parliament.uk/publications/31584/documents/177260/default/>, accessed 12 June 2026.

Different participants across the components may have distinct roles and motivations. Some may be directly responsible for operating interventions (for example, financial institutions and telco regulators) or for governing them (for example, data protection commissions and regulators), while others may play an enabling role (for example, consumer protection groups, NGOs, industry associations and academia).

© Royal United Services Institute

Experience from different jurisdictions points to the value of including actors who have aligned incentives, even if they are not the primary operators of interventions or targets of regulation. For example, 'the Philippines' fintech association actively engages with authorities on policy issues … providing inputs to the regulatory framework'.[77] Similarly, consumer protection organisations can be drivers for anti-fraud efforts and dialogue. In Pakistan, for instance, Pakistan's Network for Consumer Protection has engaged multiple regulators to address large-scale fraud, contributing to actions across financial regulation, consumer protection and enforcement.[78]

EXAMPLES **02**

Observations from a Lifecycle-Informed Approach to Participant Identification (South Africa)

- Identifies stakeholders based on their ability to act and the data they hold (for example, transactions, phone numbers and URLs), rather than sector or institutional category.
- Highlights non-traditional actors (for example, telcos, digital platforms and industry bodies) whose infrastructure is used or whose cooperation is required.
- Reveals overlaps and gaps in responsibility, supporting clearer role allocation and data-sharing design.

Note on Digital Platforms and the Tech Sector

In many countries, criminals exploit the fragmentation of the modern communications landscape itself to implement fraud campaigns, operating across multiple platforms and networks simultaneously to evade detection at any single point of oversight. Digital platforms are central to the ways in which most scams are initiated, executed and scaled. This creates a considerable structural challenge for policymakers in LMICs, as most major digital platforms implicated in scams may be headquartered in foreign jurisdictions. Even in the countries where such platforms do have a strong presence, rarely have they been held to the same standards of liability, reporting or cooperation for fraud as domestically regulated sectors such as banks and telcos.

Where fraud activity is digitally enabled, the scope for unilateral action by individual LMICs may be limited, which can make stakeholder mapping at the regional or network level particularly important.[79] Cooperation with regional partners facing similar challenges to establish a coordinated working group on scams may be a useful starting point. ASEAN's

77. Eric Duflos et al., 'Responsible Digital Finance Ecosystem (RDFE): A Conceptual Framework', September 2024, p. 22, <https://www.cgap.org/research/publication/responsible-digital-finance-ecosystem-rdfe-conceptual-framework>, accessed 12 June 2026.
78. Duflos et al., 'Responsible Digital Finance Ecosystem (RDFE)', p. 19.
79. Mark Button et al., 'Policing Cross-Border Fraud "Above and Below the Surface": Mapping Actions and Developing a More Effective Global Response', *Crime, Law and Social Change* (Vol. 83, No. 5, January 2025).

© Royal United Services Institute

Working Group on Anti-Online Scams,[80] the 2025 ASEAN Declaration on Combatting Cybercrime and Online Scams[81] and the 2026 ASEAN Guide on Anti-Scam Policies and Best Practices[82] (endorsed under the Hanoi Digital Declaration[83]) offer useful examples of such initiatives, although their efficacy in securing cooperation from the tech sector to combat scams remains to be seen.

The Global Signal Exchange,[84] launched in 2024, illustrates another emerging effort to consolidate scam-related signals across governments and participating digital platforms, including Meta and Amazon.

Enablers for Effective Implementation and Operation

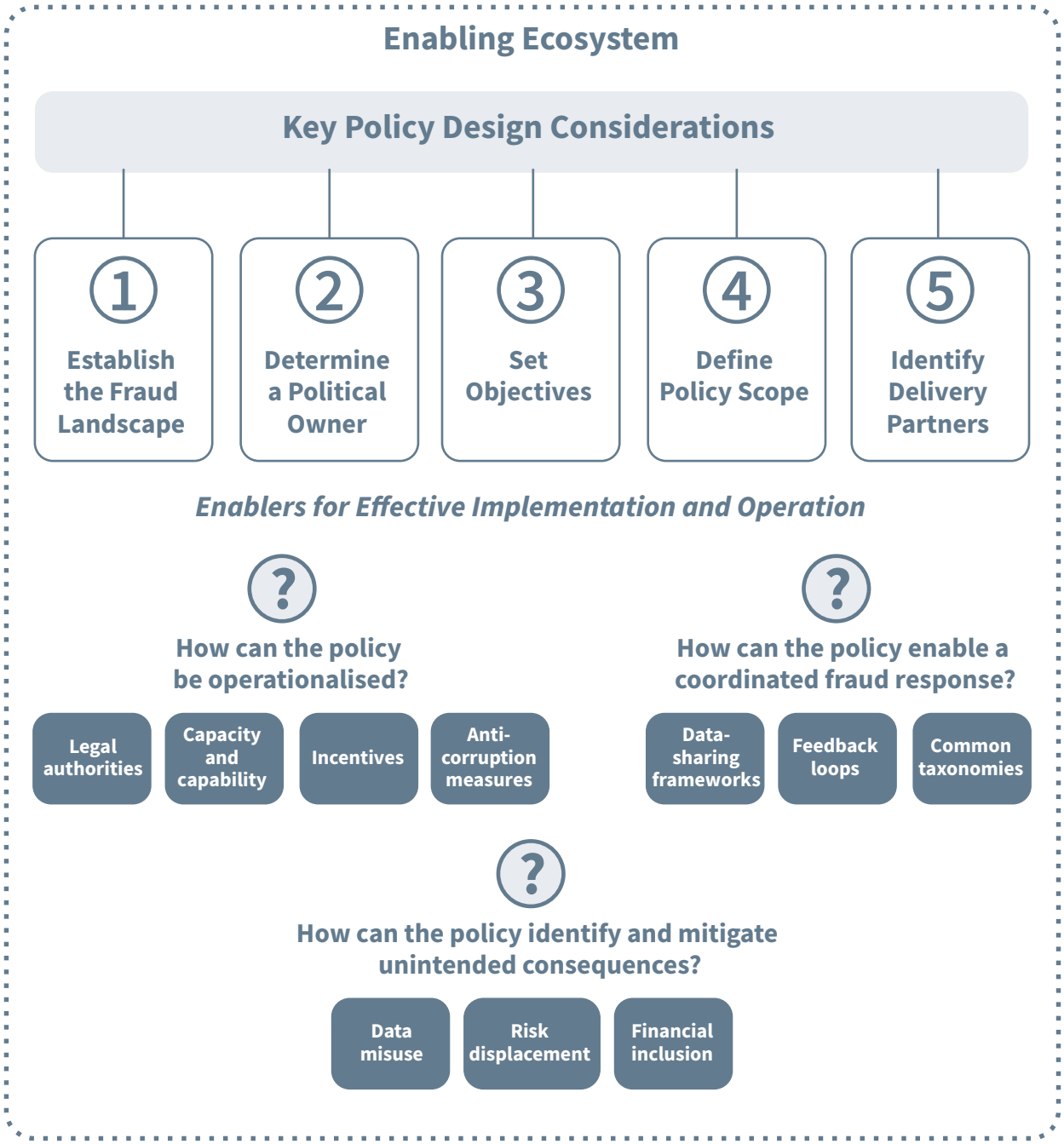
Effective implementation of fraud policy and interventions is shaped by contextual factors, including socioeconomic conditions (for example, poverty and literacy) and institutional capacity (resources), which vary across countries. Where these are insufficiently addressed, gaps can emerge between 'policy on paper' and 'policy in practice'. Rather than attempt to cover these factors exhaustively, this guide provides three analytical questions to guide implementation, drawing on research and considerations relevant to the interventions outlined in Chapter II.

- How can the policy be operationalised?
- How can the policy enable a coordinated fraud response?
- How can the policy identify and mitigate unintended consequences for consumers?

80. Southeast Asia Public Policy Institute, 'Towards an ASEAN Response to Scams', September 2025, <https://seapublicpolicy.org/wp-content/uploads/2025/09/SEAPPI_Towards-an-ASEAN-response-to-scams_September-2025.pdf>, accessed 12 June 2026.
81. ASEAN, 'ASEAN Declaration on Combatting Cybercrime and Online Scams', 2025, <https://asean.org/wp-content/uploads/2025/09/03.-ASEAN-Declaration-on-Combatting-Cybercrime-and-Online-Scams.pdf>, accessed 12 June 2026.
82. ASEAN, 'ASEAN Guide on Anti-Scam Policies and Best Practices'.
83. ASEAN, 'Hanoi Digital Declaration', January 2026, <https://asean.org/wp-content/uploads/2026/01/ADOPTED-HANOI-DIGITAL-DECLARATION_14Jan2026-CLN.pdf>, accessed 12 June 2026.
84. Global Signal Exchange, <https://www.globalsignalexchange.org/>, accessed 12 June 2026.

© Royal United Services Institute

Figure 3: Key Enablers / Questions for Effective Policy Implementation and Operation



Source: The authors.

Enabler 1: How Can The Policy Be Operationalised?

Drawing on international experience of implementing fraud policies and interventions, the authors have identified the factors enabling them to move from design to effective practice. While many such factors may exist, as a study prioritising entry-level policy design considerations, this guide focuses on whether the policy is supported by enforceable **legal authorities**, backed by sufficient **capacity and capability**, aligned with **incentives** that shape actor behaviour in line with its objectives, and resilient to practical barriers through **anti-corruption measures**.

Enabler 1.1: Legal Authorities

When designing fraud policy, countries benefit from assessing whether existing laws adequately empower stakeholders across the fraud response framework to execute their roles and whether they have the right incentives to do so. Across jurisdictions, governments are recalibrating legal frameworks to align with their evolving fraud responses. This may include expanding mandates for public and private actors or data sharing to enable the various interventions described in Chapter II. At a more foundational level, legal reforms may also be needed to ensure that authorised payment fraud and related acts are criminalised, either under existing fraud definitions or via a stand-alone offence. In cases where legal provisions originally designed for unauthorised fraud are deemed unsuitable, jurisdictions may either amend them or introduce specific provisions addressing authorised payment fraud.[85]

Consideration may also be given to whether new or expanded legal mandates are accompanied by corresponding investments in training and capacity building, specifically across law enforcement and the criminal justice system, where responses involve emerging fraud typologies, new technologies (for example, blockchain), or novel forms of digital evidence (for example, digital payment trails, platform data or device forensics).

Enabler 1.2: Capacity and Capability

Countries may benefit from considering incremental approaches to building capacity (for example, staffing, funding and infrastructure) and capability (specialist skills and expertise) alongside the design and implementation of a fraud framework, across all relevant authorities in the fraud framework: from those at the policy and criminal justice level to actors responsible for effectively operating interventions.

In practice, constraints are often managed by starting with lower-complexity interventions, relying where appropriate on stronger private sector capabilities (for example, Intervention 7),

85. See, for example, Section 4 of the Anti-Financial Account Scamming Act (2024) in the Philippines, <https://lawphil.net/statutes/repacts/ra2024/ra_12010_2024.html>, accessed 12 June 2026; Section 58AG of the Competition and Consumer Act 2010 (as amended in 2025) in Australia, <https://www.legislation.gov.au/C2004A00109/latest/text>, accessed 12 June 2026.

© Royal United Services Institute

and progressively building capability for scaling. External support can also contribute, including technical assistance, secondments and training from international donors, multilateral agencies and regional partners. For example, the World Bank has provided technical assistance, funding and training to Computer Security Incident Response Teams in 64 countries between 2014 and 2024.[86]

These considerations are also relevant to data sharing and the effectiveness of interagency or public–private partnerships (PPPs). Increased data availability does not necessarily translate into actionable intelligence without the ability of institutions to process, prioritise, analyse and act on information within operational timeframes. Thus, capacity and capability assessments may help ensure large volumes of shared data do not create additional operational pressure or risk excessive sharing of sensitive data.

Enabler 1.3: Incentives

Actors may have the capability and capacity to combat fraud but lack the incentives to act. Effective policy implementation requires actors to be motivated to achieve its objectives, and where necessary should realign incentives to ensure this. There are many ways in which actors may be incentivised (or disincentivised) to ensure desired policy outcomes, facilitate cooperation and enhance compliance (see Examples Box 3 'Motivating and Driving Implementation').

Further, Chapter II considers some mechanisms of shifting incentives as interventions in their own right, for example Intervention 6 (Harmonising the Response to Financial Losses) and Intervention 11 (Publishing Information on Entities Promoting Financial Products). While incentives are relevant across all contexts, intentionally shifting them can serve as a practical tool to combat fraud, particularly in countries where limited resources constrain investment in more complex interventions.

It is also essential, where possible, to ensure incentives are resilient to political changes, especially in contexts where changes in government may lead to wholesale policy reversal,[87] by embedding them within legal and institutional frameworks.

86. World Bank, 'Enhancing Cyber Resilience in Developing Countries', Results Brief, 29 January 2025, <https://www.worldbank.org/en/results/2025/01/29/-enhancing-cyber-resilience-in-developing-countries>, accessed 13 July 2026.
87. Author interview, online, 9 December 2025.

© Royal United Services Institute

EXAMPLES **03**

Motivating and Driving Implementation

- **Legal Mandates and Penalties**: Australia's 2025 SPF created a legal framework requiring certain business to take reasonable steps to prevent, detect, respond to and report scams, with civil penalties of up to AUD50 million in instances where they are determined to have failed to meet their obligations.[88]
- **Peer Comparisons**: Malaysia's National Fraud Portal uses peer comparison to incentivise better anti-scam performance using metrics on fraud interceptions and losses prevented.[89]
- **Collective Action**: This approach brings together competitors / actors from across society (public and private sectors) to pool intelligence and resources and encourage more impactful joint working from institutions which may otherwise operate in isolation. Indonesia's Illegal Financial Activities Eradication Task Force and its International Anti-Scam Centre unite 105 banks, 13 ministries, two authorities and six agencies, creating a collective working platform with the goal of intercepting and reducing systemic fraud loss through information sharing.[90]
- **Sharing responsibility**: This involves reallocating liability for fraud losses in a bid to prompt firms to invest in prevention and take a more proactive approach to avoid additional costs. See Intervention 6 for more information.
- **Consultation**: Bringing regulated sectors into the policy design process can give them a stake in the outcome, which incentivises constructive engagement and compliance once obligations take effect. Australia's SPF, for example, was developed through multiple rounds of public consultation.[91]
- **Good Samaritan / Safe Harbour Protections**: These are legal protections which shield actors from liability when sharing information in good faith to take action against scams. In jurisdictions where companies must navigate complex data protection rules, the Aspen Institute has proposed extending these types of liability protections to encourage a more proactive approach.[92]

Further reading: Nicolas Hocq and Vanessa Hans, *Collective Action in Practice: A Game-Changer for Business Integrity* (Basel: Basel Institute on Governance, 2025).

88. Department of the Treasury (Australia), 'Scams Prevention Framework', p. 4.
89. Author interview, online, 13 January 2026.
90. Author interview, online, 6 February 2026.
91. Daniel Mulino, 'Consulting on Industry Codes and Rules to Protect Consumers from Scams', Treasury (Australia), press release, 29 November 2025, <https://ministers.treasury.gov.au/ministers/daniel-mulino-2025/media-releases/consulting-industry-codes-and-rules-protect-consumers>, accessed 12 June 2026; Treasury (Australia), 'Scams Prevention Framework – Exposure Draft Legislation', 2024, <https://treasury.gov.au/consultation/c2024-573813>, accessed 12 June 2026.
92. Nick Bourke et al., 'United We Stand: A National Strategy to Prevent Scams', Aspen Institute Financial Security Program, 30 September 2025, p. 52, <https://www.aspeninstitute.org/publications/united-we-stand-a-national-strategy-to-prevent-scams/>, accessed 12 June 2026.

© Royal United Services Institute

Enabler 1.4: Anti-Corruption Measures

Anti-corruption measures, alongside effective AML/CFT frameworks and credible criminal laws on fraud, are a critical foundation for effective fraud policy implementation because corruption erodes trust, law enforcement credibility and system integrity.

Corruption undermines an effective fraud response in several ways. First, effective anti-fraud systems depend on people reporting scams, sharing information and engaging with authorities. Where corruption is seen as pervasive, victims are less likely to trust anti-fraud interventions or cooperate with them.[93] Second, anti-fraud frameworks rely on law enforcement credibility. If cases are not investigated or prosecuted because of corruption, institutional capture or perceived complicity, the entire framework loses legitimacy. Third, corruption can undermine the adoption of policies implemented to combat fraud. In Mexico, for example, plans to require biometric information to obtain a SIM card have been met with significant public opposition, in part driven by fears that the data collected is vulnerable to misuse given known links between security forces and organised criminals.[94] Last, tackling systemic corruption visibly is essential to set behavioural expectations on the part of the consumer. In countries with endemic corruption, studies have shown consumers may excuse small-scale fraud by pointing to high-level corruption, or view it as a lesser evil than corruption by the state.[95]

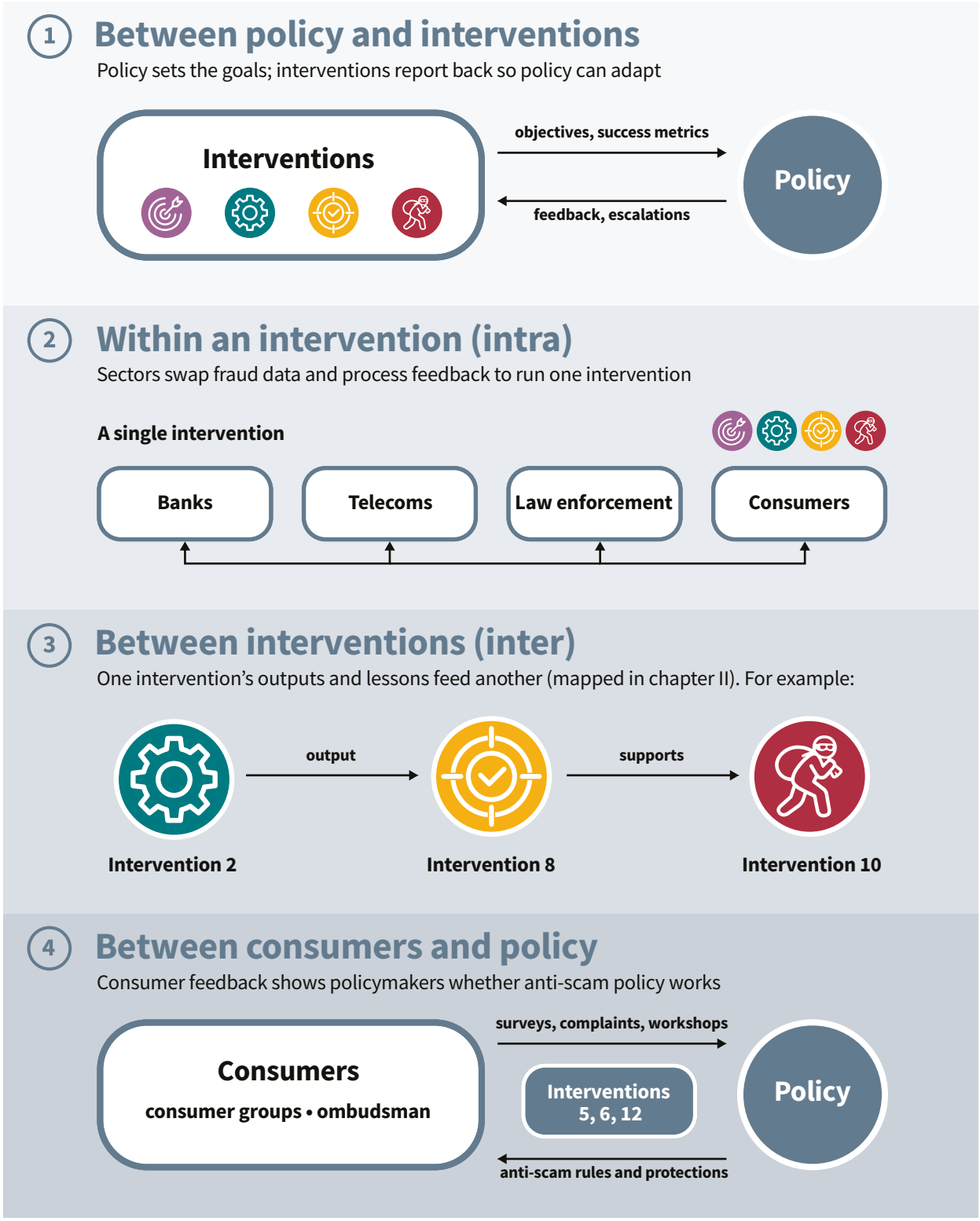
Enabler 2: How Can the Policy Enable a Coordinated Fraud Response?

A key theme emerging from this research and engagement with experts is that effective implementation depends on the extent to which different efforts and actors are able to 'talk to each other'.[96] Indeed, a successful national fraud response involves various actors and processes both at the system level (for example, fraud landscape review, policy design and regulation) and across interventions (see Figure 4).[97] This includes sharing fraud-related structured data (for example, personal data and transactions) and actionable intelligence (for example, account numbers and typologies). In addition, this could include operational information pertaining to, for example, implementation challenges, operational blockers and unstructured knowledge relating to fraud (for example, emerging change in tactics).

93. Author interview, online, 28 January 2026.
94. Author interview, online, 9 December 2025; Erica Hellerstein, 'The Mexican Government Wants to Create a Massive Database with Cell Phone Users' Biometric Data', Coda, 29 April 2021, <https://www.codastory.com/surveillance-and-control/mexico-biometric-cell-phone-law/>, accessed 12 June 2026.
95. Mark Button et al., 'Scoping Study on Fraud Centres: Ghana, India, Nigeria', Itad, May 2024, p. 46, <https://researchonline.lse.ac.uk/id/eprint/126338/1/Fraud-Scoping-Study-for-publication-2024.pdf>, accessed 12 June 2026.
96. Author interview, online, 28 January 2026.
97. Author interview, online, 28 January 2026.

© Royal United Services Institute

Figure 4: Information Flows Between Processes and Actors



Source: The authors.

Depending on context, information flows may occur across public and private sectors, between policy and interventions, across interventions, and between actors involved in the delivering each intervention. This guide draws attention to **data-sharing frameworks**, **feedback loops** and **common taxonomies** for effective and responsible data-sharing.

Enabler 2.1: Data-Sharing Frameworks

Timely data sharing, particularly cross-sector and international sharing, remains a global challenge. Barriers include the absence of clear legal provisions allowing data sharing for anti-scams purposes;[98] the fear of legal repercussions from breaching data protection frameworks (such as the General Data Protection Regulation (GDPR)) even if provisions for such data sharing exist; lack of incentives; and a lack of common taxonomies (as discussed further in Enabler 2.3, Common Taxonomies). Practical constraints also play a role, including the absence of shared infrastructure, differences in systems across industries, and the administrative and financial costs associated with establishing and maintaining data-sharing mechanisms.

International standards, such as the GDPR, require a defined purpose for sharing, an appropriate legal basis, identification of the minimum necessary data, clarity on roles and responsibilities for participating actors, and data security. Best Practice Box 1, 'Practical Considerations', outlines key practical considerations, drawing on international guidance. Strong data-protection laws and governance are essential to prevent adverse consumer outcomes, including potential misuse of data. (Data misuse is addressed separately under Enabler 3: How Can the Policy Identify and Mitigate Unintended Consequences?).

Countries are creating incentives to foster cross-sector data-sharing, including through clarifying laws and creating protections via safe harbours. For example, New Zealand has created a safe harbour to incentivise banks, telcos and digital platforms to share scams-related data quickly.[99]

98. Author interview, online, 30 January 2026.
99. Jacqueline So, 'Government Rolls Out "Safe Harbour" Legal Shield Geared Towards Addressing Online Scams', New Zealand Lawyer, 18 November 2025, <https://www.thelawyermag.com/nz/news/general/government-rolls-out-safe-harbour-legal-shield-geared-towards-addressing-online-scams/556925>, accessed 12 June 2026.

© Royal United Services Institute

BEST PRACTICE **01**

Practical Considerations

Based on international standards and literature



- Share only essential data, for example, fraudster-linked identifiers such as 'receiver account', without sharing victim information.[100]
- Use a consistent taxonomy for classifying scam-related data, to ensure uniformity in interpretation and data sharing.[101]
- Define end goals and ensure data is only used for those purposes.
- Ensure personal data is not stored for longer than needed.[102]
- Ensure mandatory escalation of data breaches within a stipulated timeframe.
- Secure data from unauthorised access or accidental loss by ensuring technology and physical access controls as necessary.[103]
- Start with a manageable framework scope as each sector and participant adds data, privacy and governance complexity. For example, Singapore's aforementioned Anti-Scam Centre was set up in 2019, with information sharing between three large banks and law enforcement.[104] This is an example of starting off with wide enough coverage with a small number of participants before expanding operations.

Further reading: Nick J Maxwell and Olivier Kraft, 'A Survey of Collaborative Analytics Platforms to Tackle Fraud', Future of Financial Intelligence Sharing, May 2026, <https://www.future-fis.com/fraudplatforms.html>, accessed 12 June 2026.

Enabler 2.2: Feedback Loops

In addition to the sharing of structured data relating to fraud, feedback could constitute practical information between different actors on outcomes (for example, how many scams were intercepted), usefulness of shared information (for example, was the scam

100. US Federal Reserve, 'Scams Information Sharing Industry Work Group Recommendations', 2023, <https://fedpaymentsimprovement.org/wp-content/uploads/scams-information-sharing-industry-work-group-recommendations.pdf>, accessed 12 June 2026; Information Commissioner's Office (ICO), 'UK GDPR Guidance and Resources: A Guide to the Data Protection Principles', <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/>, accessed 12 June 2026.
101. US Federal Reserve, 'Scams Information Sharing Industry Work Group Recommendations', p. 6.
102. ICO, 'UK GDPR Guidance and Resources'.
103. ICO, 'Security, Including Cyber Security', <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/security/>, accessed 12 June 2026.
104. Charmaine Ng, 'Police Sets Up Anti-Scam Centre, Suspicious Bank Accounts Can Now Be Frozen in a Few Days', *Straits Times*, 30 August 2019, <https://www.straitstimes.com/singapore/courts-crime/police-sets-up-anti-scam-centre-working-with-banks-to-disrupt-scammers>, accessed 12 June 2026.

© Royal United Services Institute

alert actionable?), and consumer experience (for example, do consumers find it easy to report scams to a hotline?). These loops can be direct, such as bank-to-law enforcement communication, or indirect, such as consumer perspectives reaching policymakers or firms via ombudsmen or consumer groups.

Examples of feedback loops include PPP forums, industry groups and working groups established between two or more actors, as well as cross-sector or multi-actor task forces. These may be complemented by formal escalation mechanisms and regulatory reporting lines, alongside input channels such as ombudsmen or consumer representative bodies, which provide user-level feedback into the system (see Figure 4).

Enabler 2.3: Common Taxonomies

To effectively and responsibly share information, all actors with a role in anti-fraud policies would benefit from sharing a uniform understanding of how to classify and measure fraud risk. A fraud taxonomy is a structured list of fraud types standardising this classification.

Taxonomies and thresholds enable consistent policy application, performance benchmarking and responsible data-sharing. For example, Malaysia defined a common taxonomy and harmonised fraud definitions before launching its National Fraud Portal in 2023.[105] The portal aggregates data from multiple financial firms and law enforcement and thus requires shared labels and definitions to work.

RESOURCES **02**

Defining Fraud Taxonomy

The European Banking Authority (EBA) Fraud Taxonomy provides three main considerations for determining payment fraud taxonomies:

- **Method**: how the fraudster first contacted the victim.
- **Modus**: action taken by the fraudster to trick the victim (for example, social engineering and/or account takeover).
- **Initiator**: who initiated the payment (the customer or the fraudster).

For further resources, including copies of fraud taxonomies, see Annick Moes, 'What is the EBA Fraud Taxonomy?', EBA, 20 December 2024, <https://www.abe-eba.eu/2024/12/20/what-is-the-eba-fraud-taxonomy/>, accessed 12 June 2026; and Michaela Beals, Marguerite DeLiema and Martha Deevy, 'A Framework for a Taxonomy of Fraud', Stanford Center on Longevity, July 2015, <https://www.finrafoundation.org/sites/finrafoundation/files/framework-taxonomy-fraud.pdf>, accessed 12 June 2026.

105. Author interview, online, 13 January 2025.

Enabler 3: How Can the Policy Identify and Mitigate Unintended Consequences?

Responding to fraud has the potential to reshape data flows and incentives and introduce certain levels of friction within the payments system (for example, through transaction delays or additional verification). While these are sometimes necessary to tackle fraud, they can introduce unintended effects on consumers if not actively monitored and managed.[106] These include risks to consumer protection and financial inclusion and increased risk of fraud. This section explores this further by focusing on **data sharing and scams risk**, **impacts on financial inclusion** and the potential for **risk displacement** due to behavioural adaptation by fraudsters. For each area, it sets out some practical approaches for monitoring these risks. In Chapter II, potential unintended consequences linked to individual interventions are signposted.

Enabler 3.1: Data Misuse and Heightened Scams

Data protection laws are critical to the effective implementation of fraud policy and avoiding unintended consequences of many fraud interventions outlined in Chapter II. This is because many interventions concentrate sensitive data (such as transactions, consumers, victims, fraudsters, phone numbers and digital identifiers) and create new cross-sector data flows (see for example, Intervention 15).[107] Without strong safeguards, the implementation of such initiatives can create unintended consequences, particularly by increasing the risk that consumer data collected for anti-fraud purposes is exposed to and misused by fraudsters.

An increasing number of jurisdictions are introducing national data protection regimes – setting rules for what data is sensitive, how such data is collected, used, shared and protected to safeguard individuals' rights and privacy. The GDPR and similar regimes distinguish between different categories of data including 'personal data' (for example, names and contact details) and 'sensitive personal data' (for example, biometric and financial information). These distinctions can affect the legal basis required for collection and sharing, as well as the safeguards, access controls and consent requirements that apply to them.

106. Financial Conduct Authority (FCA), 'Consumer Duty', PRIN 2A.6.2, FCA Handbook, 31 July 2023, <https://handbook.fca.org.uk/handbook/prin2a>, accessed 12 June 2026.
107. Data protection is essential society-wide and is not, by itself, specific to fraud. However, this guide focuses on how it is important in the implementation of fraud policy and interventions.

© Royal United Services Institute

Table 2: The Principles of the GDPR (Article 5)

Principle		GDPR Requirement
1	**Lawfulness, fairness and transparency**	Personal data must be 'processed lawfully, fairly, and in a transparent manner in relation to the data subject'.
2	**Purpose limitation**	Data must be 'collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes'.
3	**Data minimisation**	Data collected must be 'adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed'.
4	**Accuracy**	Personal data must be 'accurate and, where necessary, kept up to date'. Inaccurate data must be 'erased or rectified without delay'.
5	**Storage limitation**	Data must be 'kept in a form which permits identification of data subjects for no longer than is necessary' for the processing purposes.
6	**Integrity and confidentiality**	Data must be processed in a manner ensuring 'appropriate security … including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage'.
7	**Accountability**	'The controller shall be responsible for, and able to demonstrate compliance with', all of the above principles.

Source: GDPR, Article 5, 'Principles Relating to Processing of Personal Data', <https://gdpr-info.eu/art-5-gdpr/>, accessed 20 April 2026.

Aligning with standards like the GDPR, countries are creating dedicated Data Protection Authorities or Information Commissioners, while others are assigning responsibility to a central executive body such as a cabinet-level office (for example, in Kyrgyzstan) or a ministry (for example, in Cuba and Kazakhstan). Although a rare example, Mongolia splits responsibilities between its ministry of digital development and communications and the independent national human rights commission, which provides oversight.[108]

Among other roles in overseeing the implementation of data protection laws, these authorities typically receive information about data breaches within the country and have powers to investigate them and take mitigation and enforcement measures.[109]

108. DLA Piper, 'Data Protection Laws of the World', <https://www.dlapiperdataprotection.com/>, accessed 6 July 2026.
109. GDPR, Article 58, 'Powers', <https://gdpr-info.eu/art-58-gdpr/>, accessed 6 July 2026; DLA Piper, 'Data Protection Laws of the World'; Ayman Falak Medina, 'Navigating Data Protection Laws in ASEAN-6: A Guide for Foreign Investors', ASEAN Briefing, 19 December 2024, <https://www.aseanbriefing.com/news/navigating-data-protection-laws-in-asean-6-a-guide-for-foreign-investors/>, accessed 6 July 2026.

© Royal United Services Institute

Table 3: Data Protection Models

Framework	Authority	Breach Notification	Enforcement
Brazil Brazilian Data Protection Law[110]	National Data Protection Authority	Three business days[111]	• warning • tiered fines • demand erasure of data • suspension or • prohibition of data-processing activities.[112]
Nigeria Data Protection Act[113]	Nigeria Data Protection Commission	Within 72 hours	• tiered fines
Philippines Data Privacy Act[114]	National Privacy Commission	Within 72 hours	• fines and/or • imprisonment.[115]

Source: The authors, drawing on the legislation and regulator sources cited in footnotes 108–113.

RESOURCES **03**

Further Reading on Data Protection Guidance

- Privacy International, 'The Keys to Data Protection: A Guide for Policy Engagement on Data Protection', 2018, <https://privacyinternational.org/sites/default/files/2018-09/Data%20Protection%20COMPLETE.pdf>, accessed 12 June 2026.
- DLA Piper, 'Data Protection Laws of the World', <https://www.dlapiperdataprotection.com/>, accessed 12 June 2026.
- Asia-Pacific Economic Cooperation (APEC), 'APEC Privacy Framework', APEC Secretariat, 2015, <https://apec.org/docs/default-source/Publications/2017/8/APEC-Privacy-Framework-(2015)/217_ECSG_2015-APEC-Privacy-Framework.pdf>, accessed 12 June 2026.

110. Government of Brazil, 'Brazilian Data Protection Law (LGPD)', Article 55-A, last modified 23 January 2025, <https://www.gov.br/anpd/pt-br/centrais-de-conteudo/outros-documentos-e-publicacoes-institucionais/lgpd-en-lei-no-13-709-capa.pdf>, accessed 6 July 2026.
111. Machado Meyer, 'CD/ANPD RESOLUTION No. 15 OF APRIL 24, 2024', 24 April 2024, <https://www.machadomeyer.com.br/images/RESOLUCAO_CD_ANPD_N_15_DE_24_DE_ABRIL_DE_2024_eng.pdf>, accessed 6 July 2026.
112. ANPD, 'Regulation of the Enforcement Process and the Administrative Sanctioning', Resolution CD/ANPD No. 1, 28 October 2021, <https://www.gov.br/anpd/pt-br/centrais-de-conteudo/outros-documentos-e-publicacoes-institucionais/regulamento-do-processo-de-fiscalizacao-em-lingua-inglesa.pdf>, accessed 6 July 2026.
113. Federal Republic of Nigeria Official Gazette, 'Nigeria Data Protection Act, 2023', 1 July 2023, <https://cert.gov.ng/ngcert/resources/Nigeria_Data_Protection_Act_2023.pdf>, accessed 6 July 2026.
114. Government of Philippines, 'Republic Act 10173: Data Privacy Act of 2012', 15 August 2012, <https://privacy.gov.ph/data-privacy-act/>, accessed 6 July 2026.
115. National Privacy Commission (Philippines), 'Breaches', <https://privacy.gov.ph/exercising-breach-reporting-procedures/>, accessed 6 July 2026.

© Royal United Services Institute

Enabler 3.2: Risk Displacement

As with other crimes, an improved response in one area can lead to the activity shifting, rather than resulting in an overall decline (for example, 'displacement').[116] Evidence shows that when controls are strengthened against fraudulent activity, criminals often adapt quickly by moving across channels (for example, from unauthorised to authorised fraud),[117] customer segments (for example, targeting more vulnerable or less digitally literate groups), deception methods (for example, from impersonation scams to investment scams), geographically[118] (for example, from one city to another or internationally)[119] or to smaller stakeholders who are typically outside the information-sharing scope.

Monitoring for such risk displacement can happen in a few ways: through financial sector data (across payment channels and consumer segments), law enforcement data or consumer complaints or through measures listed above in Consideration 1 (for example, consumer surveys). Policymakers may prioritise monitoring known gaps, such as those identified through structured policy gap assessments, or channels and sectors not yet fully covered by existing frameworks.

Enabler 3.3: Impact on Financial Inclusion

Many anti-fraud policies and interventions induce a certain amount of friction in a consumer's financial journey,[120] and finding the right balance is a challenge each country must monitor and manage continually. Failing to tackle scams undermines trust and harms consumers, but excessive friction can deter people from accessing formal financial services. A survey in Asia, for example, found that many Malaysians will not open an account if the identity checks are too difficult or time-consuming.[121] Further, a UK-specific

116. Rob T Guerette and Kate J Bowers, 'Assessing the Extent of Crime Displacement and Diffusion of Benefits: A Review of Situational Crime Prevention Evaluations', *Criminology* (Vol. 47, No. 4, 2009), pp. 1331–68.
117. UK Finance, 'Criminals Steal Over Half a Billion Pounds and Nearly 80 Per Cent of APP Fraud Starts Online', press release, 25 October 2023, <https://www.ukfinance.org.uk/news-and-insight/press-release/criminals-steal-over-half-billion-pounds-and-nearly-80-cent-app>, accessed 12 June 2026.
118. Button et al., 'Scoping Study on Fraud Centres', pp. 38–39.
119. Interpol, 'Global Financial Fraud Threat Assessment'.
120. This guide adopts the FATF's 2025 definition of inclusion as 'access to and active use of an adequate suite of regulated, appropriate, safe, convenient and affordable financial services'. This definition not only covers barriers to onboarding (for example, KYC-driven exclusion) but also considers drivers of exclusion which may emerge through the use of financial services, such as friction at the stage of payments causing missed bills, or a loss of trust in banks and other organisations. See FATF, 'Guidance on Financial Inclusion and Anti-Money Laundering and Terrorist Financing Measures'.
121. C K Leo, 'New Trends in Payments Fraud in Asia Post-Pandemic', blog, FICO, 8 September 2022, <https://www.fico.com/blogs/payments-fraud-in-asia>, accessed 12 June 2026.

© Royal United Services Institute

study on low- and middle-income households found inconsistent implementation of interventions across the financial sector or poorly communicated consumer protection measures (such as increased account security) undermine consumer trust in digital financial products.[122]

FATF has recognised that overly restrictive controls may contribute to financial exclusion and potentially increase money laundering risks by pushing activity outside regulated channels.[123] Thus, where fraud controls create barriers to legitimate participation, there may be implications for both inclusion and wider AML/CFT objectives. Considerations around proportionality, the handling of false positives, and the availability of effective redress mechanisms are important in managing trade-offs between effective fraud prevention and avoiding undue harm to financial participation. This is particularly relevant where interventions such as restricted databases (see Intervention 2), payment-risk monitoring (for example, Intervention 8), and automated fraud detection standards may generate false positives that affect legitimate users, for example through delayed transactions or temporary service restrictions.

Drawing from literature on consumer-focused initiatives and policy development, Table 4 provides examples of methods that policymakers can use to assess impact, monitor and evaluate fraud policy and interventions for indications of unintentional exclusion. Adopting these methods for monitoring inclusion would require setting metrics that go beyond fraud losses and funds recovered to include consumer outcomes. Recommendations from international consumer-focused organisations suggest governments work with consumer groups and industry to ensure scam protections do not lead financial services providers to view vulnerable consumers as too risky or too costly to serve.[124]

122. Arzu Abbasova and Poornima Subramaniam, 'The Impact of Fraud on Financial Inclusion in the UK', *RUSI Research Papers* (May 2026), <https://www.rusi.org/explore-our-research/publications/research-papers/impact-fraud-financial-inclusion-uk>, accessed 12 June 2026.
123. FATF, 'Guidance on Financial Inclusion and Anti-Money Laundering and Terrorist Financing Measures'.
124. Consumers International, 'Stopping Online Scams and Building Consistency and Coordination for Consumers', March 2026, p. 30, <https://www.consumersinternational.org/media/699948/consumers-international-stopping-online-scams-building-consistency-and-coordination-for-consumers.pdf>, accessed 12 June 2026.

© Royal United Services Institute

Table 4: Methods for Assessing And Monitoring Unintended Consequences

Method	Policy Implementation Stage		Case Study
	Impact Assessment Before Implementation	Monitoring After Implementation	
Public Consultations	✓	✓	Singapore solicited feedback through a public consultation, in October 2023, over its proposed Shared Responsibility Framework before adopting it.[125]
Consumer Surveys	✓	✓	The Central Bank of Kenya uses consumer surveys across several functions: industry surveys of supervised institutions to assess AML/CFT preventive measures, and the FinAccess household survey – conducted jointly with the Kenya National Bureau of Statistics and Financial Sector Deepening Kenya – to measure financial inclusion, including uptake of digital financial services.[126]
Key Performance Indicators (KPIs)	✓	✓	The BNR in Rwanda sets annual KPIs aligned with its strategic plan, tracking insurance penetration as well as coverage among women, youth and urban versus rural populations.[127]
Thematic Reviews		✓	Multi-firm thematic reviews are a core part of the UK financial regulator's supervision, used to monitor existing measures, outcomes and emerging risks.[128]
Tiered Licensing	✓		In 2025, Kenya proposed a draft tiered licensing model for non-deposit-taking digital lenders, where larger firms meet stricter requirements to curb fraud and protect consumers.[129]
Regulatory Sandboxes	✓		Regulators worldwide have adopted sandboxes to create flexible, evidence-based environments for testing new technologies or policies. In 2025, for example, São Tomé and Príncipe launched a sandbox to test new digital financial services and identify risks before they reach the market.[130]
Social Media Monitoring		✓	Ireland's Central Bank monitors social media to track consumer concerns. Insights from expressions of dissatisfaction and public conversations feed into periodic risk assessments and firm engagements.[131]

125. Monetary Authority of Singapore, 'Consultation Paper on Proposed Shared Responsibility Framework', P016-2023, 25 October 2023, <https://www.mas.gov.sg/publications/consultations/2023/consultation-paper-on-proposed-shared-responsibility-framework>, accessed 6 July 2026.
126. Cenfri, 'Regulating and Enabling Innovation: R3LAB Toolkit', June 2024, p. 17, <https://fsdafrica.org/wp-content/uploads/2024/08/24-08-19-R3Lab-Regulating-for-Innovation-Toolkit.pdf>, accessed 6 July 2026.
127. *Ibid*.
128. FCA, 'Supervision', updated 24 February 2026, <https://www.fca.org.uk/about/how-we-regulate/supervision#thematic-reviews>, accessed 6 July 2026.
129. Streamline, 'CBK Drafts Tiered Oversight to Rein in Digital Lenders and Protect Consumers', 11 August 2025, <https://streamlinefeed.co.ke/news/cbk-drafts-tiered-oversight-to-rein-in-digital-lenders-and-protect-consumers>, accessed 6 July 2026.
130. World Bank, 'Global Experiences from Regulatory Sandboxes', Fintech Note No. 8, 2020, <https://documents1.worldbank.org/curated/en/912001605241080935/pdf/Global-Experiences-from-Regulatory-Sandboxes.pdf>, accessed 6 July 2026.
131. Central Bank of Ireland, 'Social Media Monitoring', 2026, <https://www.centralbank.ie/regulation/consumer-protection/compliance-monitoring/social-media-monitoring>, accessed 8 July 2026.

© Royal United Services Institute

RESOURCES **04**

Tools to Design Impact and Monitoring Assessment

- Ivo Jeník and Schan Duff, 'How to Build a Regulatory Sandbox: A Practical Guide for Policy Makers', September 2020, <https://www.cgap.org/research/publication/how-to-build-regulatory-sandbox-practical-guide-for-policy-makers>, accessed 12 June 2026.
- Cenfri, 'Regulation and Enabling Innovation: R3LAB Toolkit'.
- CGAP, 'Market Monitoring Tools', <https://www.cgap.org/topics/collections/market-monitoring-tools>, accessed 12 June 2026.
- Gabriel Kwok Hui Chen and Araz Taeihagh, 'Designing Regulatory Sandboxes: A Comprehensive Framework for Aligning Functionalities and Objectives', *Policy Design and Practice* (Vol. 9, No. 1, 2026), pp. 1–15.
- Sophie Sutcliffe and Julius Court, 'A Toolkit for Progressive Policymakers in Developing Countries', Overseas Development Institute, January 2006, <https://media.odi.org/documents/190.pdf>, accessed 12 June 2026.

A system-level approach to fraud policy design mitigates the risk of fragmented responses across actors, supports the development of a shared strategic vision, facilitates stakeholder buy-in and helps ensure policy objectives are operationally viable. Furthermore, effective policy implementation relies on various, context-dependent considerations pertaining to legal frameworks, structural incentives and operational considerations. Last, responding to fraud also requires ongoing monitoring and mitigation of unintended consequences. Ongoing efforts include monitoring behavioural adaptations (by consumers or fraudsters) that may displace risk rather than reduce it, the impacts on financial inclusion, and increased exposure to scams arising from the misuse of data shared through fraud prevention mechanisms.

© Royal United Services Institute

Intervention Design

An effective response to fraud relies on a web of interrelated interventions that may each serve multiple objectives. This chapter examines fraud interventions, setting out their main objectives and how they help tackle fraud. For each intervention type, it outlines design and operational considerations with practical examples. Last, it calls out examples of feedback loop dependencies and potential unintended consequences. Readers can connect these interventions back to effective implementation considerations in Chapter I, whether by approaching the topic from a top-down system design perspective or by mapping interventions to effective implementation considerations.

Scope and Taxonomy

This guide's set of interventions reflects the practice of global anti-fraud efforts as described in existing surveys[132] and interviews conducted as part of this research. It does not include interventions addressing contextual factors, such as levels of corruption and poverty. The response to these contextual factors is itself complex and beyond the scope of this guide. However, anti-fraud strategies should acknowledge dependencies on poverty-reduction or anti-corruption efforts and involve relevant stakeholders.

The 15 intervention cards are organised around specific sub-objectives of anti-fraud efforts. For ease of use, the cards are designed to have minimal overlap (although they should be interlinked in practice) and maximum coverage (although more interventions are likely to exist or emerge in the future).

Developing a taxonomy requires finding a common denominator between disparate initiatives. As such, the term 'intervention' should be read to refer to an overarching intervention type. The diversity of examples within each intervention card illustrates the range of implementation options, as well as the possibility for countries to scale their response over time.

132. See, for example, World Bank, 'Fraud Risks in Fast Payments' , focus note, October 2023, <https://fastpayments.worldbank.org/sites/default/files/2023-10/Fraud%20in%20Fast%20Payments_Final.pdf>, accessed 12 June 2026; Hooper, Banner and Chew, 'Anti-Scam Handbook, v2.0'; UNODC, 'Public-Private Partnership Toolkit Against Organized Fraud', 2026, <https://www.unodc.org/res/organized-crime/GFS/publications/UNODC_Public-Private_Partnership_Toolkit_Against_Organized_Fraud_EN.pdf>, accessed 12 June 2026.

© Royal United Services Institute

Other surveys tend to group interventions into clusters or pillars, for example based on a criminal response cycle or the required medium (technological or regulatory).[133] However, since the organisation of national anti-fraud efforts depends on each jurisdiction's existing frameworks, this chapter follows a different approach to maximise flexibility.[134] Interventions are listed in alphabetical order, with each intervention card identifying characteristics that may be used by policymakers to organise their national strategies.

Intervention Characteristics

Each intervention is presented via a dedicated intervention card. The cards are not intended as a detailed review of each intervention, but an overview to help policymakers map out potential areas for intervention; decide on suitability, cost and prioritisation of interventions; and identify resources for further reading. The characteristics described in each intervention card are as follows:

Fraud Chain Component Targeted

As discussed in Chapter I, most fraud operations rely on a combination of fraud chain components, such as: preparation/infrastructure, initiation, execution and extraction. In practice, fraud components may overlap and require a joint response. Notwithstanding this caveat, the primary fraud component(s) targeted by a given intervention clarifies which stakeholders are most critical to its implementation. The intervention cards can also be used to map out interventions deployed in a jurisdiction and identify gaps in coverage.

Preventive or Reactive Nature

Measures can be classified according to whether their primary function is to *prevent* fraud-related events or rather to *react* to such events, whether attempted, suspected or confirmed. This distinction applies within each of the fraud chain components identified above. Depending on the fraud chain component, the fraud-related event to be prevented or addressed may be the sale of stolen data, the impersonation of a trusted institution or a misdirected payment.[135]

The split between preventive and reactive measures is not binary. Anti-fraud measures operate on a continuum, with reactive measures feeding directly into future preventive measures. For example, effective victim support in response to one event has a key role to play in preventing revictimisation.

133. World Bank, 'Fraud Risks in Fast Payments', p.9.
134. UNODC, 'Organized Fraud'.
135. See, for example, Hooper, Banner and Chew, 'Anti-Scam Handbook, v2.0', p. 68. The handbook makes a similar distinction between proactive and reactive measures. Unlike this guide, it presents the occurrence of a scam (rather than the detection of a wider range of fraud-related events) as the trigger for reactive measures.

© Royal United Services Institute

Other Characteristics

In addition to the two dimensions above, the intervention cards list other factors that can determine an intervention's suitability, feasibility, cost and effectiveness. These factors, which are discussed in more detail where most relevant, include:

- legal and operational dependencies that can help countries prioritise those interventions for which the dependencies are less onerous or already met;
- the availability of international standards or implementation frameworks countries can or should follow when designing an intervention; and
- criminal adaptation and other potential unintended consequences, as discussed in Chapter I. These risks do not reduce the suitability of an intervention. Indeed, risk displacement can be seen as a sign that an intervention is serving its purpose in disrupting the criminal methods. However, the risks of unintended consequences are highlighted to help authorities anticipate and monitor them, and adapt efforts as needed.

Key for Fraud Chain Components



Note: the intervention types are listed in alphabetical order, not by order of importance.

© Royal United Services Institute

INTERVENTION **01**

Adapting the Law Enforcement and Criminal Justice Response





Reactive

Description and Key Design Considerations

Jurisdictions are adjusting the law enforcement and criminal justice response to match the complexity and speed of fraud. While the exact design of this response varies significantly depending on each jurisdiction's legal and institutional set-up, adaptation efforts cover:

- **Legal and operational powers**: This includes amending legislation (use of digital evidence and establishing jurisdiction over cases in which the victim is abroad), creating specialised agencies or courts,[1] granting additional powers to law enforcement (for example, an administrative power to suspend transactions prior to a freezing or restraint order), or allowing for cooperation with relevant private sector stakeholders.
- **International cooperation**: With most fraud cases having a cross-border dimension, international cooperation is essential to enable the successful investigation, prosecution and adjudication of fraud cases. International cooperation relies on bilateral,[2] regional[3] and global arrangements (see examples below).
- **Tackling proceeds**: Due to the volume of criminal proceeds generated by fraud, and the challenges in identifying or prosecuting perpetrators, AML tools (including financial investigations, seizures and confiscations) and their effective use are central to counter-fraud efforts.[4]
- **Alternative mechanisms**: Due to limitations in the capacity of the criminal justice system to deal with increasing fraud volumes, civil law mechanisms such as administrative fines, dissolution orders, bans or sanctions regimes are under consideration as alternative measures where appropriate.[5]
- **Visibility**: National authorities interviewed for this research consider publicly communicating law enforcement actions, and building public confidence in the response, to be key to encouraging fraud victims to file reports.[6]

International standards or initiatives	**Examples** • **Standards**: UN Convention against Cybercrime,[7] FATF Recommendations[8] • **Initiatives**: Financial Crime Analysis File (FinCAF), Interpol Silver Notices, I-GRIP[9], Operation HAECHI[10]
Dependencies	• international cooperation • legal gateways to support cross-agency and public–private collaboration
Links with other interventions	• most effective when combined with Intervention 15 • provides input for Intervention 4 • uses output from Intervention 5 and Intervention 13
Additional resources	• UNODC, 'Organized Fraud'; UNODC, 'Public-Private Partnership Toolkit Against Organized Fraud'; UNODC and Interpol, 'Call to Action on Combating Fraud', Global Fraud Summit, 2026, <https://www.unodc.org/res/organized-crime/GFS/Global-Fraud-Summit-Outcome-Documents-English.pdf>, accessed 12 June 2026

© Royal United Services Institute

INTERVENTION **02**

Building and Maintaining Restricted Databases of Fraud-Related Events, Perpetrators and Vectors



Preventive

Description and Key Design Considerations

Databases of fraud-related events are used or under discussion in most countries. Most tend to focus on known perpetrators or vectors of fraud, to prevent a perpetrator identified by one service provider from shifting their activities to another one (for example, in Nigeria[11]). A smaller number of initiatives are considering victim-related data to address repeat victimisation.[12]

Due to the sensitivity of fraud-related data and the need for trust among participants, most initiatives begin with a small set of features and a limited group of institutions at the domestic level (for example, a consortium of financial institutions or telco companies). However, cross-sector and cross-border initiatives are emerging (see examples below and listed in 'Additional Resources').

Privacy-enhancing technologies allow banks to determine whether a new customer matches a watchlist of another bank, without disclosing the full list (for example, in Mexico[13]).

International standards or initiatives	• Global Signal Exchange (global database of URLs and other data points associated with fraud)[14] • Cifas International Fraud Data Standard (under development)[15] • INTERPOL I-Checkit database of Stolen and Lost Travel Documents[16]
Dependencies	• trust among stakeholders • alignment with data protection legislation (see Chapter I) • evidentiary standards and legal redress routes for individuals who consider they were wrongly included on a database or whose name triggers a false positive[17] • reliable and consistent identification
Links with other interventions	• provides input for Intervention 8 and Intervention 10 • most effective when combined with Intervention 13
Unintended consequences to mitigate and monitor	• financial exclusion (see Chapter I) • risk of data leaks or misuse (see Chapter I) • risk of displacement to non-participants
Additional resources	• Maxwell and Kraft, 'A Survey of Collaborative Analytics Platforms to Tackle Fraud'; Association of Certified Anti-Money Laundering Specialists, 'Cross-Sector Fraud Information Sharing: Pathways to Action', white paper, March 2026, <https://www.acams.org/sites/default/files/2026-03/ACA1836_Cross-Sector%20Fraud%20Information%20Sharing_Pathways%20to%20Action_White%20Paper_v3.pdf>, accessed 12 June 2026

© Royal United Services Institute

INTERVENTION **03**

‘Designing Out’ Fraud



Preventive

Description and Key Design Considerations

Making products and services less susceptible to fraud by design is a core part of efforts to tackle risks upstream, given the challenges of downstream detection and incident response. In addition to each institution’s efforts to mitigate the criminal exploitation of its **products**, today’s fraud techniques require a cross-sector response. For example, preventing digital wallet fraud requires multiple sectors, including financial institutions and mobile phone manufacturers, to collaborate.[18]

As speed is a key element of fraud tactics, protective measures may introduce friction in certain **services**. For example, certain jurisdictions are introducing cooling-off periods, imposing a minimum time lapse between the addition of a new payee and a first transfer (for example, in Mexico[19] and Brazil[20]). These measures can also be introduced on a voluntary basis, allowing consumers to opt into additional protections[21] or out of certain higher-risk services that they do not need (for example, inbound calls originating from abroad[22]).

International standards or initiatives	• International industry bodies such as the GSMA[23] and the International Banking Federation[24] provide guidance on safe product and service design.
Dependencies	• Certain measures may require a legal or regulatory basis or are most effective when mandated at a sector level.
Links with other interventions	• informed by outputs of Intervention 1, Intervention 4, Intervention 13 • complemented by Intervention 10, Intervention 13
Unintended consequences to mitigate and monitor	• Protective product- or service-level features can create friction for customers, which needs to be balanced against the socioeconomic benefits of fast payments (see Chapter I).
Additional resources	• Australian Payments Network, ‘Safety by Design in Payment Systems’, July 2025, <https://auspaynet.com.au/sites/default/files/2025-08/Payment%20Safety%20by%20Design%20LRS%20Taskforce%20V1_FINAL%20VERSION.pdf>, accessed 12 June 2026; World Bank, ‘Fraud Risks in Fast Payments’

© Royal United Services Institute

INTERVENTION **04**

Disrupting Criminal Infrastructure

Preventive and Reactive

Description and Key Design Considerations

Disruption efforts seek to degrade criminal networks by targeting their business model and operational capabilities. The elements of the criminal infrastructure that national authorities can disrupt depend on the jurisdiction's risk profile (specifically, the extent to which fraud actors use infrastructure located in or managed from the jurisdiction) as well as its ability to act against infrastructure components located abroad. Disruption efforts include:

- **action against scam compounds**: Interpol Operation Storm Makers,[25] international sanctions against a company operating scam centres[26];
- **restrictions on SIM cards**:[27] biometric identification requirements for SIM cards (Mexico)[28], prohibition of SIM farms (UK),[29] cross-sector action against pay-as-you-go SIMs (UK)[30]; and
- **action against online infrastructure supporting scams**: dissemination of indicators of compromise linked to a company alleged to provide infrastructure for fraudulent websites (US).[31]

International standards or initiatives	**Examples:** • Global Fraud Taskforce 'Operation Shadow Storm' (launched in March 2026)[32] • Operation 'Breaking Chains'[33] • Operation FRONTIER+[34]
Dependencies	• jurisdiction over infrastructure or, alternatively, cooperation from relevant governments • engagement with additional sectors such as domain name system (DNS) registrars and service providers
Links with other interventions	• relies on intelligence obtained across all other interventions, especially Intervention 1, Intervention 9 and Intervention 15
Unintended consequences to mitigate and monitor	• Measures tackling the criminal use of equipment such as SIM cards (for example, via biometric identification) can lead to data misuse of legitimate users. See Chapter I.
Additional resources	• ASEAN, 'ASEAN Guide on Anti-Scam Policies and Best Practices'

© Royal United Services Institute

INTERVENTION **05**

Encouraging Consumers and Businesses to Report Fraud Events

Link between preventive and reactive measures

Description and Key Design Considerations

Reporting channels serve not only as a trigger for reactive measures, but also as a key source of data that helps public and private stakeholders adapt their fraud response and measure impact. Yet, fraud is universally considered to be under-reported. Based on available literature and interviews conducted for this research, key design considerations for reporting channels include:

- **Ease of access**: A common goal is to make it easy for consumers or businesses to know where to report fraud. Certain jurisdictions have promoted a single number, app or website as the overarching reporting channel.[35] In cases in which multiple routes are available, jurisdictions have adopted a 'no-wrong-door' approach, allowing victims to file their report regardless of the route they choose.[36]
- **Ease of use**: Interviewees emphasised the importance of making the experience pain-free.[37] This includes efficiency (for example, the use of an AI agent for collecting and preprocessing reports, availability of alternative formats such as voice message, channels for automated reporting by businesses) as well as the absence of judgement.
- **Feedback loop**: Several interviewees indicated that consumers are more likely to report fraud if they are confident that their report will be acted on.[38]
- **Fraud reports from abroad**: To support the rapid recovery of funds and prosecution in cross-border cases, certain fraud portals allow foreign victims to file a report in the country in which they believe the fraud originated.[39]
- **Recognition**: Many reporting portals seek to remove the shame associated with victimisation by emphasising that reports protect others and support anti-fraud stakeholders.[40]

International standards or initiatives	• The Global Anti-Scam Alliance launched the portal <www.scam.org> in March 2026 to help fraud victims identify the correct reporting channel.
Dependencies	• capacity to deal with fraud reports and update victims, including in cases in which their report may not meet the definition of fraud • strong data security, as fraudsters often revictimise targets by pretending to offer support in recovering funds
Links with other interventions	• to be promoted via Intervention 12 • to be informed by Intervention 14
Unintended consequences to mitigate and monitor	• An effective reporting system is likely to attract a growing number of reports, including bogus reports filed by criminals.[41] The rapid increase and inconsistent relevance of fraud reports should be anticipated.

© Royal United Services Institute

INTERVENTION **06**

Harmonising the Response to Financial Losses

Reactive

Description and Key Design Considerations

Industry-wide dispute resolution protocols harmonise how service providers respond to cases of authorised payment fraud. They level the playing field for customers, reduce the harm to victims (in case of reimbursement) and incentivise service providers to invest in effective preventive measures (when integrated into liability frameworks). Protocols have been introduced on a voluntary or mandatory basis. Key design considerations for dispute resolution protocols include:

- **What fraud typologies are covered**: Certain protocols apply to all typologies of authorised payment fraud (such as in the UK[42] and New Zealand[43]), whereas others are limited to specific typologies, such as impersonation-based scams (for example, in the EU[44] and Singapore[45]).
- **What are each party's obligations**: To achieve consistency in dispute resolutions, regulations or codes of conduct should clarify the obligations of financial institutions related to fraud prevention and detection.[46] They may also address standards of care expected from customers, or obligations applicable to other sectors such as telecommunications.[47]
- **Who covers the loss**: Dispute resolution protocols address not only whether a customer can claim a reimbursement, but also how the cost is shared between service providers, for example between the sending and the receiving bank, or between a bank and a telecommunications company in the case of bank impersonation scams.

International standards or initiatives	• No established standard or initiative exists. Current dispute resolution protocols apply only to domestic payments. However, certain jurisdictions are discussing bilaterally how to facilitate cross-border reimbursements via Memorandums of Understanding.
Dependencies	• clear industry or regulatory framework clarifying respective obligations and liability of service providers (assigning liability for loss across all industry sectors in the fraud chain may only be possible with new cross-sector agreements or laws) • financial and technical capacity within affected sectors to process claims • oversight mechanisms to handle any legal challenges (for example, ombudsman)
Links with other interventions	• builds on Intervention 5 • informed by Intervention 13
Unintended consequences to mitigate and monitor	• Without appropriate safeguards, reimbursement schemes can lead to a rise in first-party fraud. However, experience from the UK does not suggest that this risk has materialised to date.
Additional resources	• Payment Systems Regulator, 'APP Scams Reimbursement: Consolidated Policy Statement'

© Royal United Services Institute

INTERVENTION **07**

Leveraging AML Measures Taken by Regulated Entities

Preventive and Reactive

Description and Key Design Considerations

In line with international standards, financial institutions and other designated sectors are required to apply preventive and reactive measures under AML regulations in nearly all jurisdictions. AML measures have helped detect and tackle financial flows linked to fraud via, for example, the identification and reporting of unusual account activity[48] or the suspension of transactions (where permitted).[49]

Financial institutions have adjusted AML practices to address fraud-related ML typologies, especially the use of money mules. This includes updates to onboarding practices and ongoing account monitoring based on those typologies. This also requires a shift towards real-time capabilities to match the speed of financial flows.

International standards or initiatives	• FATF Recommendations (especially Recommendations 9–25)[50] • FATF, Egmont Group and Interpol guidance on cyber-enabled fraud (2023)[51] and FATF 2026 update[52] • Egmont BEC Project Team (established protocols between law enforcement and financial intelligence units (FIUs), and between international FIUs to follow and freeze BEC proceeds)[53]
Dependencies	• adoption and implementation of AML laws and regulations in line with FATF standards • reliable identification of individual and legal entities
Links with other interventions	• uses output from Intervention 2 • most effective when combined with Intervention 15
Unintended consequences to mitigate and monitor	• Risk displacement to less regulated sectors, including virtual assets • Exclusion of legitimate customers whose profile or behaviour may be similar to money mules • Risk of tipping off
Additional resources	• Westmore and Owen, ‘Following the Fraud’

© Royal United Services Institute

INTERVENTION **08**

Monitoring Payment Risk Via Inter-Institutional Systems



Preventive

Description and Key Design Considerations

Inter-institutional cooperation improves or supplements fraud monitoring solutions that financial institutions can apply individually *prior to authorising a payment*.

In most cases, these systems are designed to reveal fraud risks that institutions may not be able to detect using only the data they hold. In jurisdictions where institutions' fraud controls are less mature, a centralised system can also help harmonise controls while reducing the cost for individual participants.[54]

Inter-institutional fraud risk monitoring systems vary in terms of centralisation. Certain systems involve an entity (such as a payment system operator) that monitors transactions and assigns risk scores based on data from all participants. By contrast, other systems rely on bilateral sharing of information between institutions, for example, sharing of risk information between the sending and receiving institution (through payment messages or through other secure channels[55]).

While inter-institutional collaboration efforts were originally sector-specific, examples of cross-sector prepayment collaboration are emerging. For example, a financial institution can use an API to verify in real time whether a customer making a payment is on the phone, and if so whether the call was inbound and how long it lasted, which significantly improves the accuracy of fraud risk assessments.[56] In addition, a consortia of financial institutions leverage privacy-enhancing technologies to build joint monitoring systems without sharing the underlying customer data.

International initiatives	• Pilot projects are seeking to facilitate cross-border prepayment information sharing.[57]
Dependencies	• trust among stakeholders • alignment with data protection legislation (see Chapter I) • Standard Operating Procedure, possibly involving a central party to avoid a web of bilateral arrangements • communication channels to share risk data prepayment, including from the receiving institution to the sending institution
Links with other interventions	• builds on Intervention 13 • supports Intervention 10
Unintended consequences to mitigate and monitor	• risk displacement to institutions and sectors that are not involved
Additional resources	• Maxwell and Kraft, 'A Survey of Collaborative Analytics Platforms to Tackle Fraud'

© Royal United Services Institute

INTERVENTION **09**

Proactively Identifying and Restricting Fraud Vectors





Preventive

Description and Key Design Considerations

While defensive measures are meant to detect fraud as and when it reaches a potential victim, public and private stakeholders are increasingly seeking to *proactively* identify and restrict fraud vectors. Identification efforts include monitoring public platforms or infiltrating private social media channels to identify potential fraudulent schemes, including ads by unlicensed providers in jurisdictions that have licensing regimes.[58]

Other recent initiatives leverage data from multiple sectors, achieving a significant uplift in the number of fraud vectors identified (for example, telephone numbers, accounts, URLs).[59]

Depending on the nature and location of the fraud vector, measures taken to restrict the associated harm include regulatory enforcement, reporting to web hosts or social media platforms, or blocking access to a webpage (when takedown is not possible). In addition, AI-based 'honey traps' are used to either waste fraudsters' resources[60] or collect intelligence on them.[61]

Dependencies	• sufficient information and incentives for social media companies (or other relevant service providers) to act on reports • for multiparty initiatives: alignment with data protection legislation (see Chapter I) • empowering private sector stakeholders to adopt a proactive approach, including via Good Samaritan protections (see Chapter I)
Links with other interventions	• provides input to Intervention 1, Intervention 2, Intervention 4 and Intervention 11
Unintended consequences to mitigate and monitor	• Risk displacement: fraudsters evade scrutiny by requesting victims to move to more opaque communication channels (see Chapter I).

© Royal United Services Institute

INTERVENTION **10**

Providing Customers with Counterparty Information

Preventive

Description and Key Design Considerations

These interventions seek to equip service users with more information on an individual counterparty to help them better protect themselves.

At the **initiation stage**, many service providers have adopted proactive measures to alert customers to communications or platforms (using phone calls, SMS, email and/or websites) that may be linked to scams. Other measures seek to improve information on the origin of calls, including by requesting providers to label calls originating from abroad.[62]

Counterparty information is also increasingly provided at the **payment stage**. Thanks to confirmation of payee (CoP) systems, a person or business making a payment can verify if the name linked to the beneficiary account aligns with the name of the intended recipient.[63] By reducing the risk of misdirected payments, CoP systems are particularly relevant in the context of fraud types that involve impersonation, such as business email compromise. While initial data from the UK suggests that CoP has helped reduce certain types of fraud among early adopters,[64] the evidence of CoP impact on system-wide fraud levels remains limited.

International standards or initiatives	• CoP is one of the implementation options provided for under FATF Recommendation 16. Guidance on the implementation of Recommendation 16 is due to be published in late 2026.
Dependencies	• While certain mechanisms can be implemented by individual service providers, more advanced ones such as CoPs may require adjustments to messaging protocols to allow a sending institution to obtain information from the receiving institution (either via a directory or bilaterally).
Links with other interventions	• uses output from Intervention 2, Intervention 11 and Intervention 13 • to be explained via Intervention 12
Unintended consequences to mitigate and monitor	• risk displacement to institutions and sectors that are not involved[65] • repeated warnings that are not sufficiently linked to the nature of a transaction can lead to 'message fatigue'
Additional resources	• Lipis Advisors, 'Best Practices in Directory Models', August 2023, <https://cdn.prod.website-files.com/5c47368cf83b6b677da3c7db/64d4da0389a18f6835f93d2b_Part1-BP.pdf>, accessed 12 June 2026; Lipis Advisors, 'Part Two: Best Practices in Directory Models', November 2023, <https://cdn.prod.website-files.com/5c47368cf83b6b677da3c7db/65524bd74ab0af260d346ef0_Part%20two_Best%20practices.pdf>, accessed 12 June 2026; P20, 'Payee Verification: Overview of Approaches Used by Credit-Push Payment Systems', interim report, June 2020, <https://static1.squarespace.com/static/5efcc6dae323db37b4d01d19/t/5fd184b0ad61ab583182c558/1607566513047/P20+Regulation+WG+Interim+Report+-+Payee+Verification+-+June+2020.pdf>, accessed 12 June 2026

© Royal United Services Institute

INTERVENTION **11**

Publicising Information on Registration Status or Past Misconduct of Entities Promoting Financial Products

Preventive (investment scams)

Description and Key Design Considerations

With investment scams considered as one of the most common fraud typologies in many countries,[66] governments have introduced or tightened registration / licensing requirements for business or individuals promoting financial products (including so-called 'finfluencers'). The **registration status** can help investors make informed decisions, provided it is public and actively used by the public.

Public information on an entity's **past misconduct** can also protect future investors. However, fraud is most often perpetrated by short-lived organisations that are set up for criminal purposes and dissolved within a short time, which can limit the efficacy of public lists of bad actors.[67]

Information may be accessible via a public list, a hotline and/or a chatbot.[68]

International standards or initiatives	• IOSCO I-SCAN: a global portal maintained by the International Organization of Securities Commissions (IOSCO) listing firms that are the subject of an alert or warning[69]
Dependencies	• resources needed to maintain the information and address any legal challenges from listed individuals or entities
Links with other interventions	• most effective when combined with Intervention 5 • to be explained via Intervention 12 • uses output from Intervention 9 • provides input for Intervention 10
Unintended consequences to mitigate and monitor	• Ineffectiveness: The sense of trust associated with an entity's addition on a list can be exploited by fraudsters impersonating the said entity. A list that is not sufficiently maintained can be misleading for consumers who rely on it to make decisions. • Risk displacement to products that lie outside the regulatory perimeter (for example, spirits or other high-value goods[70])

© Royal United Services Institute

INTERVENTION **12**

Raising Awareness on Scam Methods, Scale and Consequences



Preventive

Description and Key Design Considerations

Most awareness-raising campaigns are meant to help potential fraud targets to not only defend themselves but also know what to do in case of victimisation (for example, in Singapore[71]). This includes all types of victimisation, ranging from financial abuse to recruitment as a money mule and coercion into committing fraud. Certain awareness-raising campaigns are aimed at businesses[72] or other stakeholders such as frontline staff and carers who can help safeguard potential victims.

The channel and communication style are adapted to each type of victimisation and demographic. Scam awareness apps, podcasts, browser extensions, chatbots and other interactive formats play an increasing role in driving ongoing engagement (for example, campaigns delivered via interactive voice response games).[73] This is complemented by offline communications to reach rural or older populations.[74]

Certain community-based campaigns seek to change social attitudes towards fraud, including by involving victims.[75] This can help address both the stigma faced by victims and the cultural acceptance of fraud as a means of survival. See, for example, volunteer watchers (Philippines),[76] Scam Marshals (UK)[77] and National Scam Survivor Day (US).[78]

While awareness-raising campaigns are one of the most common anti-fraud intervention, studies show that not all of them increase scam identification ability and that prior testing is essential to cost effectiveness.[79]

International standards or initiatives	• UNODC, Handbook on Effective Communication Strategies for the Prevention of Organized Fraud (2026)[80] • UNODC Organized Crime Strategy Toolkit for Developing High-Impact Strategies[81] • UNODC Trapped in Scam Crime Campaign[82]
Dependencies	• coordination among public and private stakeholders to deliver a consistent message • availability of funding and methods to test awareness campaigns and confirm their effectiveness prior to a launch
Links with other interventions	• most effective when combined with Intervention 5 • complements Intervention 14 (to prevent revictimisation)

Unintended consequences to mitigate and monitor	• Among other effects, ill-designed awareness campaigns can:
	  • discourage consumers from engaging with the formal financial system;
	  • lead consumers to overestimate their ability to spot scams, including when campaigns are focused on individual methods and out of sync with new trends; and
	  • reinforce stigma among victims if they suggest that fraud victimisation is a sign of negligence.

© Royal United Services Institute

INTERVENTION **13**

Setting Standards for Entity-Level Detection and Incident Response

Preventive and Reactive

Description and Key Design Considerations

As customers alone cannot be expected to recognise increasingly sophisticated forms of fraud, detection efforts by the industry are considered one of the most essential interventions.[83] Industry standards are emerging as a key driver in all relevant sectors, via regulatory requirements[84] as well as voluntary initiatives.[85] They define not only preventive measures to detect fraud attempts, but also the reactive measures to be taken when a fraud-related event is suspected or identified.[86] Reactive measures can include:

- in the **telecommunication or social media sectors**: blocking an inbound communication,[87] informing the customer that a communication was stopped;
- in the **financial sector**: suspending a transaction, informing the receiving financial institution that a suspicious transaction was stopped; or
- **across sectors**: securing digital evidence, reporting fraud events to a regulator, providing victim support.

Given the rapidly evolving nature of fraud methods, industry standards are supported by training[88] or sector-wide (or consortium-level) information sharing on best practices.

International standards or initiatives	• FATF Recommendation 16 was revised in 2025 to strengthen the obligation of financial institutions to detect misdirected payments. • GIRAF, a global forum for telecom regulators, is developing a framework of harmonised regulatory recommendations.[89] • International industry bodies such as the GSMA or the International Banking Federation provide guidance on fraud detection methods.[90]
Dependencies	• the fact that certain measures require a legislative or regulatory basis and appropriate integration with the payment network • technical and human capacity to implement standards • empowering private sector stakeholders to improve their detection efforts, including via Good Samaritan protections (see Chapter I)
Links with other interventions	• most effective when combined with Intervention 2 and Intervention 8 • complemented by Intervention 10 (as additional protection) and Intervention 6 (as incentive)
Unintended consequences to mitigate and monitor	• Financial exclusion (see Chapter I): more advanced analytics and information sharing can reduce the rate of false positives and therefore the impact on legitimate customers. • The cost can place a high burden on smaller providers or market entrants, including those offering services to underserved groups. Shared anti-fraud utilities can help reduce the cost.
Additional resources	• P20, 'Best Practice Approaches for Combating Payee Scams', May 2021, <https://www.payments20.com/news/p20-scams-report>, accessed 12 June 2026; ASEAN, 'ASEAN Guide on Anti-Scam Policies and Best Practices'

INTERVENTION **14**

Supporting Victims





Preventive and Reactive

Description and Key Design Considerations

While a detailed review of victim support practices is beyond the scope of this guide, the factors shaping initiatives reviewed for this research include:

- **Diversity of forms of victimisation**: All stages of the fraud chain can involve various forms of victimisation that each require different responses in addition to psychological support, for example, physical protection and reintegration for individuals coerced into committing fraud,[91] identity repair for those deceived to act as money mules, or financial compensation for victims of extortion.
- **Multifaceted harm**: While repairing the financial harm is often the initial priority in the case of financial abuse, support services seek to address many other dimensions of harm, including long-term trauma and mental health impact. The variety of victim support programmes, including community-based support[92] and support for fraud victims who experienced identity theft,[93] reflects the multifaceted nature of the harm and the needs of victims.
- **Tackling stigma**: There is a growing body of research indicating that effective victim support requires a shift in how fraud victims are perceived and perceive themselves. Various victim-support initiatives promote language that does not implicitly blame or dehumanise the victim,[94] also learning lessons from other types of abuse (including domestic abuse). See additional resources listed below.

Emerging literature and pilot programmes in the UK highlight the role of victim-support measures, such as access to safe lending and support for managing debt incurred through fraud, in stabilising victims' financial situations and reducing their vulnerability to further exploitation.

Dependencies	• understanding of prevalent forms of victimisation in the jurisdiction and associated harms • sufficient confidentiality and data security to prevent the misuse of data for revictimisation
Links with other interventions	• should inform the design of Intervention 5 and Intervention 12
Additional resources	• Providing support to fraud and scams victims – a toolkit for practitioners: Keith Brown, Elizabeth Carter and Jennifer Hawkswood, 'Coercion and Control in Financial Abuse: Learning from Domestic Abuse', National Trading Standards Scams Team, <https://www.friendsagainstscams.org.uk/mint-project/uploads/630378746.pdf>, accessed 12 June 2026 • Michael Skidmore et al., 'Invisible Harms: Understanding the Hidden Health Impact of Fraud', Police Foundation, 17 February 2026, <https://www.police-foundation.org.uk/publication/invisible-harms-understanding-the-hidden-health-impact-of-fraud/>, accessed 12 June 2026 • AARP and FINRA Foundation, 'Blame and Shame in the Context of Financial Fraud: A Movement to Change our Societal Response to a Rampant and Growing Crime', June 2022, <https://bbbmarketplacetrust.org/wp-content/uploads/2025/03/FINRA-AARP-Research.pdf>, accessed 12 June 2026

© Royal United Services Institute

INTERVENTION **15**

Tracing Fraud Proceeds and Communications Via Multiparty Collaboration






Reactive

Description and Key Design Considerations

To enable an effective response, countries are developing national capabilities that support real-time information sharing on fraud events.

In the financial sector, these mechanisms (often referred to as anti-scam centres) support the tracing of funds through the financial system, and possibly their freezing, and have helped deprive criminals of their proceeds and return funds to victims.[95] Examples include Anti-Scam Centres in Hong Kong [96], Singapore,[97] Malaysia[98] and Indonesia.[99]

Pending the implementation of a real-time tracing capability, certain jurisdictions have taken interim measures to expedite communications between law enforcement and financial institutions, or among financial institutions, such as a directory of fraud focal points to be contacted,[100] a mechanism for joint investigation, or a crisis room co-locating bank officers from different banks. In South Africa, financial institutions established a crisis room to track fraud proceeds across institutions. The proof-of-concept led to a 30–40% increase in recovery, supporting the business case for automation.[101]

In the telecom sector, industry-wide efforts aim to facilitate traceback (identifying the origin of fraudulent calls).

International standards or initiatives	• One Consortium International Traceback working group (part of the Restore Trust Initiative): industry-wide effort to improve traceback of fraudulent calls[102] • Interpol guidance on anti-scam centres[103]
Dependencies	• trust among system participants and low level of insider risk • alignment with data protection legislation (see Chapter I) • Standard Operating Procedure • effective and secure communication channels to share data in real time • capacity and legal authority of institutions to act quickly
Links with other interventions	• most effective when combined with Intervention 1 • supports Intervention 4 and Intervention 14 (in case of recovery of funds) • uses output from Intervention 5 and Intervention 13
Unintended consequences to mitigate and monitor	• risk displacement to institutions and sectors that are not involved
Additional resources	• Maxwell and Kraft, 'A Survey of Collaborative Analytics Platforms to Tackle Fraud'

© Royal United Services Institute

Conclusion

The implications of authorised payment fraud extend well beyond individual financial loss. Left unchecked, it erodes trust in institutions, strains law enforcement and threatens to reverse the financial inclusion gains which many low- and middle-income countries have worked hard to secure in recent decades. Should fraud continue to evolve apace, economic stability and the integrity of the financial system itself could be placed in severe jeopardy.

Meeting this threat effectively requires countries to move beyond a patchwork of isolated measures towards a coordinated response. As most modern fraud campaigns operate across sectors, channels and borders, an effective response must also reach across siloes. As such, this guide seeks to provide policymakers with a structured means of considering national anti-fraud policy at the system level. Chapter I sets out the key design considerations and enabling conditions on which an effective response depends, and Chapter II profiles 15 interventions, broken down by characteristics which allow policymakers to assess the measures most likely to be feasible and have impact in their own context.

© Royal United Services Institute

About the Authors

Georgia Jones is a Research Analyst at the Centre for Finance and Security at RUSI, specialising in the design and effective implementation of financial crime policy, with an emphasis on fraud. Her research examines how anti-financial crime frameworks perform in practice in the UK and internationally. She leads the Centre's international fraud portfolio, which supports policymakers in low- and middle-income countries to develop contextually relevant anti-fraud policies.

Olivier Kraft has contributed to global efforts against financial crime across the public, private and non-profit sectors, and specialises in the interactions between financial crime and new technologies. His experience includes supporting countries in the implementation of the UN Convention Against Corruption, advising the World Bank's Sanctions Board on allegations of fraud, and assessing the effectiveness of national anti-money laundering systems. As a Research Fellow at RUSI, he designed and led the Financial Crime 2.0 programme and published the first comprehensive review of how governments can leverage advanced analytics for AML purposes; he has since led a global bank's intelligence assessment on virtual currencies and worked with technology companies developing AI-led solutions for financial crime detection.

Poornima Subramaniam is an expert in financial crime, technology and policy. She began her career in the defence sector specialising in open source intelligence before moving into banking, where she led an investigations team within HSBC's Global Financial Crime Investigations function. Over the past two years as a consultant, she has focused on data-driven research, advisory and advocacy. Her focus areas include detection controls, payments fraud and effective implementation of public digital infrastructure underpinning financial crime frameworks.

© Royal United Services Institute

Annex 1: Interventions by Component and Primary Function

	Description	Fraud chain				Prevent	React
01	Adapting the law enforcement and criminal justice response	✓	✓	✓	✓		✓
02	Building and maintaining restricted databases of fraud-related events, perpetrators and vectors	✓	✓	✓		✓	
03	'Designing out' fraud		✓	✓		✓	
04	Disrupting criminal infrastructure	✓				✓	✓
05	Encouraging consumers and businesses to report fraud events		✓	✓		✓	✓
06	Harmonising the response to financial losses			✓			✓
07	Leveraging AML measures taken by regulated entities				✓	✓	✓
08	Monitoring payment risk via inter-institutional systems			✓		✓	
09	Proactively identifying and restricting fraud vectors		✓			✓	
10	Providing customers with counterparty information		✓	✓		✓	
11	Publicising information on registration status or past misconduct of entities promoting financial products		✓			✓	
12	Raising awareness on scam methods, scale and consequences	✓	✓	✓	✓	✓	
13	Setting standards for entity-level detection and incident response		✓	✓		✓	✓
14	Supporting victims	✓	✓	✓	✓	✓	✓
15	Tracing fraud proceeds and communications via multiparty collaboration			✓	✓		✓

© Royal United Services Institute

Annex 2: Navigating This Guide

The tables below map common policymaker questions to where they are addressed in this paper.

Getting Started	
Developing an anti-fraud response, irrespective of resource endowment	
As a less digitally mature economy	**Chapter 1:** all five Key Policy Design Considerations apply regardless of digital / economic development; Define Policy Scope (start where structures exist) **Interventions 1, 4, 7, 12 and 14:** interventions which probably require the least amount of institutional / legal reform in most contexts
Assessing the fraud landscape	**Chapter 1:** Establish the Fraud Landscape; Box 1 (survey tools); Identify Delivery Partners (gather evidence from multiple stakeholders)
Understanding who is affected	**Chapter 1:** Set Objectives (victim harm); Impact on Financial Inclusion **Intervention 14:** forms of victimisation, multifaceted harm, stigma
Defining priorities	**Chapter 1:** Define Policy Scope; Establish the Fraud Landscape **All intervention cards:** list prerequisites and dependencies to help policymakers assess their feasibility
Securing buy-in for the anti-fraud agenda	**Chapter 1:** Set Objectives (anchoring to existing national priorities); Establish the Fraud Landscape (building an evidence base); Determine a Political Owner (signalling prioritisation).

Tailoring the Response	
Shaping the institutional arrangements and incentives needed to operationalise an effective approach	
Assigning liability and mobilising partners	**Chapter 1:** Identify Delivery Partners **Interventions 6 and 13:** loss allocation frameworks; setting standards for detection efforts
Engaging telcos and digital platforms	**Chapter 1:** Define Policy Scope; Identify Delivery Partners **Interventions 4, 9, 10, 12 and 13** disruption; restriction of fraud vectors; counterparty information; raising awareness; setting detection standards
Enabling data-sharing	**Chapter 1:** How Can the Policy Enable a Coordinated Fraud Response? **Interventions 2, 8 and 15:** databases; prepayment information sharing; tracing
Setting up reporting mechanisms	**Chapter 1:** Feedback Loops; Identify Delivery Partners **Interventions 5 and 13:** victim reporting; setting detection standards

© Royal United Services Institute

Ensuring Efficacy	
Ensuring anti-fraud initiatives are achieving positive change in the short and long term	
Measuring impact	**Chapter 1:** Set Objectives; Common Taxonomies; Feedback Loops **Interventions 2, 5, 8 and 13:** restricted database; victim reporting; prepayment information sharing; setting detection standards
Monitoring for risk displacement	**Chapter 1:** Risk Displacement; Enabler 3: How Can the Policy Identify and Mitigate Unintended Consequences? **All intervention cards:** unintended consequences sections

© Royal United Services Institute

Endnotes

1 Specialised Commercial Crimes Courts (South Africa), for more information see: Antony Altbeker, 'The Specialised Commercial Crime Court', SA Crime Quarterly, No. 2, November 2002, p. 31, <https://journals.co.za/doi/pdf/10.10520/EJC47588>, accessed 1 July 2026.

2 Home Office, 'Statement of Intent Between the UK and the Republic of Nigeria on Co-operation Relating to Cyber-Enabled Fraud and Scams', 19 March 2026, <https://www.gov.uk/government/publications/statement-of-intent-on-co-operation-on-cyber-enabled-fraud-and-scams/>, accessed 12 June 2026; Home Office, 'MoU Between the Government of the United Kingdom and the Socialist Republic of Vietnam on Cooperation to Combat the Threat of International Fraud', 3 November 2025, <https://www.gov.uk/government/publications/memorandum-of-understanding-on-the-threat-of-international-fraud/>, accessed 12 June 2026.

3 Singapore Police Force, 'Operation FRONTIER+: A Unified Front Against Transnational Scams', Police Life, 18 August 2025, <https://www.police.gov.sg/Media-Hub/Police-Life/2025/08/Operation-FRONTIER-A-United-Front-Against-Transnational-Scams>, accessed 12 June 2026; Europol, 'European Cybercrime Centre – EC3', <https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3>, accessed 12 June 2026.

4 FATF, 'Cyber-Enabled Fraud: Digitalisation and Money Laundering, Terrorist Financing and Proliferation Financing Risks'.

5 UK Government, *Fraud Strategy 2026–2029*, p.50; Button et al., 'Policing Cross- Border Fraud "Above and Below the Surface"', p.5.

6 Author interviews, online,13 January and 20 January 2026.

7 UN Convention against Cybercrime, adopted by the General Assembly of the United Nations on 24 December 2024, <https://www.unodc.org/unodc/en/cybercrime/convention/home.html>, accessed 29 June 2026.

8 FATF, 'The FATF Recommendations', as amended June 2026, <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html>, accessed 29 June 2026.

9 Interpol, 'Global Financial Fraud Assessment', May 2024, p. 19, <https://www.interpol.int/en/News-and-Events/News/2026/INTERPOL-report-warns-of-increasingly-sophisticated-global-financial-fraud-threat>, accessed 12 June 2026.

10 Interpol, 'USD 439 Million Recovered in Global Financial Crime Operation' [Operation HAECHI VI], press release, 24 September 2025, <https://www.interpol.int/News-and-Events/News/2025/USD-439-million-recovered-in-global-financial-crime-operation>, accessed 12 June 2026.

11 Central Bank of Nigeria, 'Revised Regulatory Framework for Bank Verification Number (BVN) Operations and Watch-List for the Nigerian Banking Industry', 12 October 2021, <https://www.cbn.gov.ng/Out/2021/CCD/REVISED%20REGULATORY%20FRAMEWORK%20FOR%20BANK%20VERIFICATION%20NUMBER%20(BVN)%20OPERATIONS%20AND%20WATCH-LIST%20FOR%20THE%20NIGERIAN%20BANKING%20INDUSTRY%20121021%20FINAL.pdf>, accessed 12 June 2026.

12 Author interview, online, 17 February 2026; Cifas, 'APP Victim Check', <https://www.cifas.org.uk/fraud-prevention-community/combined-threat-protect/app-victim-check>, accessed 12 June 2026.

13 Veradat, <https://veradat.com/>, accessed 12 June 2026.

14 Global Signal Exchange, <https://www.globalsignalexchange.org/>, accessed 12 June 2026.

15 Cifas, 'A Global Policy Framework for Tackling Fraud and Scams', March 2026, <https://www.cifas.org.uk/global_policy_framework>, accessed 12 June 2026.

© Royal United Services Institute

16 The access used to be limited only to the aviation industry but has since been expanded to financial institutions to prevent fraudsters opening bank accounts using fake documents to launder criminal proceeds.

17 Cifas, 'National Fraud Database Principles', <https://www.cifas.org.uk/fraud-prevention-community/member-benefits/data/nfd/nfd-principles>, accessed 12 June 2026.

18 UK Government, *Fraud Strategy 2026–2029*.

19 Banco de México, 'Information for SPEI® users', <https://www.banxico.org.mx/services/interbanking-electronic-payme.html>, accessed 12 June 2026.

20 Fernanda Curti, 'BCB Normative No. 491: How Brazil Can Strengthen Pix Fraud Prevention', blog, Feedzai, 18 December 2024, <https://www.feedzai.com/blog/bcb-normative-no-491-how-brazil-can-strengthen-pix-fraud-prevention/>, accessed 12 June 2026.

21 Cifas, 'I Want to Apply for Protective Registration', 2026, <https://www.cifas.org.uk/pr>, accessed 12 June 2026.

22 Ministry of Digital Development and Information (Singapore), 'Anti-Scam Efforts', last updated 14 April 2026, <https://www.mddi.gov.sg/other-pages/anti-scam-efforts/>, accessed 12 June 2026.

23 GSMA, 'Scams Content Hub', 2026, <https://www.gsma.com/solutions-and-impact/technologies/security/scams/scams-content-hub/>, accessed 29 June 2026.

24 Paul Benda, 'Fraud and Scams TF', IBFed Fraud and Scams Task Force, <https://www.ibfed.org.uk/working-groups/corporate-governance-wg/>, accessed 29 June 2026.

25 Interpol, 'INTERPOL Operation Reveals Further Insights into "Globalization" of Cyber Scam Centres', press release, 8 December 2023, <https://www.interpol.int/en/News-and-Events/News/2023/INTERPOL-operation-reveals-further-insights-into-globalization-of-cyber-scam-centres>, accessed 23 July 2026.

26 US Department of the Treasury, 'U.S. and U.K. Take Largest Action Ever Targeting Cybercriminal Networks in Southeast Asia', press release, 14 October 2025, <https://home.treasury.gov/news/press-releases/sb0278>, accessed 12 June 2026.

27 For more examples, see ASEAN, 'Guide on Anti-Scam Policies and Best Practices', January 2026, <https://asean.org/wp-content/uploads/2026/01/ASEAN-Guide-on-Anti-Scam-Policies-and-Best-Practices-090126.pdf>, accessed 12 June 2026.

28 Author interview, online, 9 December 2025; Hellerstein, 'The Mexican Government Wants to Create a Massive Database with Cell Phone Users' Biometric Data'.

29 Department for Science, Innovation and Technology, *Government Response to the Consultation 'Preventing the Use of SIM Farms for Fraud*, CP 978 (London: The Stationery Office, November 2023).

30 Stop Scams UK, 'UK Dismantles Organised Crime Infrastructure in Fight Against Fraud', 9 March 2026, <https://stopscamsuk.org.uk/uk-dismantles-organised-crime-infrastructure-in-fight-against-fraud/>, accessed 12 June 2026.

31 Federal Bureau of Investigation, 'FBI Flash: Infrastructure Used to Manage Domains Related to Cryptocurrency Investment Fraud Scams Between October 2023 and April 2025', IC3, 29 May 2025, <https://www.ic3.gov/CSA/2025/250529.pdf>, accessed 12 June 2026.

32 Home Office, 'Global Taskforce Launched to Hunt Down Overseas Scammers'.

33 Korea.net, 'Police Agency, Interpol Host Transnational Crime Event in Seoul', 10 June 2026, <https://www.korea.net/NewsFocus/policies/view?articleId=293812>, accessed 29 June 2026.

34 Singapore Police Force, 'Operation FRONTIER+'.

35 For examples, see author interview with staff of national hotline in the Philippines, online, 25 November 2025; author interview with staff of harmonised fraud contact number for retail banking customers in the UK, online, 29 January 2026.

36 National Anti-Scam Centre (Australia), 'Quarterly Update: July to September 2023', 27 November 2023, <https://www.nasc.gov.au/reports-and-publications/quarterly-update/nasc-quarterly-update-july-september-2023>, accessed 3 July 2026. The update states that one of its principles is 'helping consumers find the answers and support they need wherever they report'.

37 Author interviews, online, 20 January and 17 February 2026.

38 Author interviews, online, 20 January, 30 January and 28 January 2026.

39 Author interview, online, 20 February 2026 (citing Hong Kong and Singapore as examples).

40 For examples, see Canada's Fraud Reporting Service homepage. Government of Canada, 'Report Cybercrime and Fraud', <https://reportcyberandfraud.canada.ca/>, accessed 12 June 2026; AARP Fraud Watch Network™ Helpline, <https://www.aarp.org/money/scams-fraud/helpline/>, accessed 12 June 2026.

41 Author interview, online, 17 February 2026.

42 Payment Systems Regulator, 'APP Scams Reimbursement: Consolidated Policy Statement', May 2025, <https://www.psr.org.uk/media/rhelv4op/ps25- 5-app-scams-reimbursement-consolidated-policy-statement-may-2025.pdf>, accessed 12 June 2026.

43 New Zealand Bankers' Association, 'Banks Step Up Customer Scam Protections and Compensation', press release, 23 April 2025, <https://nzba.org.nz/banks-step-up-customer-scam-protections-and-compensation>, accessed 12 June 2026.

44 European Parliament and Council of the European Union, 'Regulation on Payment Services', *Official Journal of the European Union*, 2023, Article 59, <https://eur-lex.europa.eu/resource.html?uri=cellar:04cc5bd5-196f-11ee-806b-01aa75ed71a1.0001.02/DOC_1&format=PDF>, accessed 12 June 2026.

45 Monetary Authority of Singapore, 'Guidelines on Shared Responsibility Framework'.

46 Voluntary code of conduct holding a financial institution liable for reimbursement if it failed to implement five defined consumer protection measures (New Zealand); see New Zealand Bankers' Association, 'Banks Step Up Customer Scam Protections and Compensation'; Guidelines of the Central Bank of Nigeria on APP fraud (in draft at time of writing): Central Bank of Nigeria, 'Exposure Draft of the Guidelines for Handling Authorised Push Payment Fraud'.

47 Monetary Authority of Singapore, 'Guidelines on Shared Responsibility Framework'.

48 See, for example, the case of a suspicious transaction report leading to the identification of a money mule network used to launder more than $95.2 million of criminal proceeds derived from fraud: Egmont Group, 'Best Egmont Cases: Financial Analysis Cases 2021–2023', 2024, pp. 32–33, <https://egmontgroup.org/wp-content/uploads/2024/09/EGMONT_2021-2023-BECA-III_FINAL.pdf>, accessed 12 June 2026.

49 FATF, Egmont Group and Interpol, 'Illicit Financial Flows from Cyber-Enabled Fraud', p. 54.

50 FATF, 'The FATF Recommendations'.

51 FATF, Egmont Group and Interpol, 'Illicit Financial Flows from Cyber-Enabled Fraud'.

52 FATF, 'Cyber-Enabled Fraud'.

53 FATF, Egmont Group and Interpol, 'Illicit Financial Flows from Cyber-Enabled Fraud', p. 55.

54 See, for example, Nigeria Inter-Bank Settlement System, 'NIBSS: Digital Payment Fraud Drops 51% to ₦25.85b in 2025', <https://nibss-plc.com.ng/nibss-digital-payment-fraud-drops-51-to-%E2%82%A625-85b-in-2025/>, accessed 13 July 2026; PayInc (formerly BankservAfrica, South Africa), 'Business Report 2025', pp. 23–24, <https://businessreports.payinc.co.za/pdf/PayInc_Business_Report_2025.pdf>, accessed 13 July 2026; National Payments Corporation of India, 'Fraud Risk Management', <https://www.npci.org.in/who-we-are/risk-management/fraud-risk-management>, accessed 13 July 2026.

55 For example, BioCatch, 'Trust', <https://www.biocatch.com/trust>, accessed 12 June 2026.

56 Andrew Wooden, 'GSMA and UK Finance Team Up for API-Based Anti-Fraud Initiative', *Telecoms.com*, 5 November 2024, <https://www.telecoms.com/security/gsma-and-uk-finance-team-up-for-api-based-anti-fraud-initiative>, accessed 12 June 2026.

© Royal United Services Institute

57 Duality Technologies, 'Case Study: Duality Enables Cross Border Collaboration to Accelerate the Fight Against Financial Crimes', February 2024, <https://dualitytech.com/wp-content/uploads/2024/02/FINAL-Duality-IMDA-MC-Case-Study-Feb-2024.pptx-1.pdf>, accessed 12 June 2026.

58 See, for example, the AI surveillance tool deployed by the Securities and Exchange Board of India to detect unlicensed actors offering financial advice on social media: Aayushi Chaubey, 'SEBI Removes 1.2 Lakh Misleading Finfluencer Posts Using AI Surveillance Tool "Sudarshan"', Angel One, updated 2 March 2026, <https://www.angelone.in/news/market-updates/sebi-removes-1-2-lakh-misleading-finfluencer-posts-using-ai-surveillance-tool-sudarshan>, accessed 12 June 2026.

59 Stop Scams UK, 'Meta and Stop Scams Members Announce FIRE Expansion', 25 September 2024, <https://stopscamsuk.org.uk/meta-and-stop-scams-members-announce-fire-expansion/>, accessed 12 June 2026.

60 Virgin Media O2, 'O2 Unveils Daisy, the AI Granny Wasting Scammers' Time', 14 November 2024, <https://news.virginmediao2.co.uk/o2-unveils-daisy-the-ai-granny-wasting-scammers-time/>, accessed 12 June 2026.

61 Apate.ai, <https://www.apate.ai>, accessed 12 June 2026.

62 Federal Communications Commission, 'Ninth Further Notice of Proposed Rulemaking (FNPRM) FCC 25-76', October 2025, <https://docs.fcc.gov/public/attachments/FCC-25-76A1.pdf>, accessed 12 June 2026.

63 Payment Systems Regulator, 'Response to Our Call for Views CP21/6', October 2021, p. 12, <https://www.psr.org.uk/media/ktonkca3/psr-rp21-1-confirmation-of-payee-response-paper-oct-2021.pdf>, accessed 12 June 2026.

64 Payment Systems Regulator, 'Confirmation of Payee: Requirements for Further Participation in CoP', May 2022, p. 5, <https://www.psr.org.uk/media/gc1bfva1/psr-cp22-2-confirmation-of-payee-requirements-for-further-participation-in-cop.pdf>, accessed 12 June 2026.

65 Payment Systems Regulator, 'Confirmation of Payee: Call for Views', May 2021, p. 18, <https://www.psr.org.uk/media/ehfnk4qh/cp21-6-confirmation-of-payee-call-for-views.pdf>, accessed 12 June 2026.

66 Interpol, 'Global Financial Fraud Threat Assessment'.

67 Author interviews, online, 9 December 2025 and 20 January 2026.

68 ChongLuaDao, <https://chongluadao.vn>, accessed 12 June 2026.

69 International Securities & Commodities Alerts Network (I-SCAN), <https://www.iosco.org/i-scan/>, accessed 29 June 2026.

70 Author interview, online, 18 December 2025.

71 Long-term national campaign emphasising key steps, including the importance of reporting fraud. See Singapore Police Force and National Crime Prevention Council (Singapore), 'I Can ACT [Add, Check, Tell] Against Scams Resource Guide', <https://file.go.gov.sg/resourceguidepamphleteng.pdf>, accessed 12 June 2026.

72 Cellule de Renseignement Financier (Luxembourg), 'Trend Alert #2: Business Email Compromise (BEC) Targeting the Investment Sector', trend alert, November 2025, <https://crf.public.lu/dam-assets/news/trend-alert-2-bec.pdf>, accessed 12 June 2026.

73 Rafe Mazer, 'How Interactive Storytelling Is Protecting Ugandans from Mobile Money Fraud', Innovations for Poverty Action, 28 March 2025, <https://poverty-action.org/how-interactive-storytelling-protecting-ugandans-mobile-money-fraud>, accessed 12 June 2026.

74 Author interview, online, 25 November 2025.

75 UNODC, 'Survivor-Informed Action Brief on Preventing and Combating Fraud', <https://www.unodc.org/res/organized-crime/GFS/publications/UNODC_Survivor-informed_action_brief_on_combating_fraud.pdf>, accessed 12 June 2026.

76 Jocel De Guzman, 'A Grounded Approach to Scam Prevention in the Philippines', Tech for Good Institute, 26 January 2026, <https://techforgoodinstitute.org/insights/country-spotlights/a-grounded-approach-to-scam-prevention-in-the-philippines/>, accessed 12 June 2026.

© Royal United Services Institute

77 Friends Against Scams, 'Fed Up With Scams? Become a Scam Marshal', <https://www.friendsagainstscams.org.uk/mint-project/uploads/143406943.pdf>, accessed 12 June 2026.

78 BBB Marketplace Trust, 'National Scam Survivor Day', <https://bbbmarketplacetrust.org/scam-survivor/>, accessed 12 June 2026.

79 Elif Kubilay et al., 'Can You Spot a Scam? Measuring and Improving Scam Identification Ability', *Journal of Development Economics* (Vol. 165, No. 103147, October 2023).

80 UNODC, 'Handbook on Effective Communication Strategies for the Prevention of Organized Fraud', 2026, <https://www.unodc.org/res/organized-crime/GFS/publications/UNODC_Handbook_on_Effective_Communication_Strategies_for_the_Prevention_of_Organized_Fraud_EN.pdf>, accessed 12 June 2026.

81 UNODC, 'Organized Crime Strategy Toolkit for Developing High-Impact Strategies', 2021, <https://www.unodc.org/cld/uploads/pdf/Strategies/OC_Strategy_Toolkit_Ebook.pdf>, accessed 29 June 2026.

82 UNODC, '#TrappedInScamCrime Regional Campaign', <https://www.unodc.org/roseap/en/TrappedInScamCrime/index.html>, accessed 29 June 2026.

83 Mark Button et al., 'Practitioner Perspectives on What Works in Preventing Fraud Against Older Adults', *Journal of Economic Criminology* (Vol. 12, No. 100213, June 2026).

84 See, for example, mandatory industry codes of conduct to be introduced under Australia's Scams Prevention Framework: Australian Treasury, 'Scams Prevention Framework', 3 February 2025, <https://treasury.gov.au/publication/p2025-623966>, accessed 3 July 2026.

85 See, for example, the fraud prevention seal issued by an industry body (Brazil): Federação Nacional das Instituições de Pagamento, 'Fin Launches New Stage of the Fraud Prevention Seal and Expands Initiative to New Segments', 17 November 2025, <https://www.ecommerceupdate.com.br/en/fin-lanca-nova-etapa-do-selo-de-prevencao-a-fraudes-e-amplia-iniciativa-para-novos-segmentos/>, accessed 12 June 2026.

86 See, for example, a protocol advising branch staff on how to detect and respond to potential fraud (UK): House of Lords Fraud Act 2006 and Digital Fraud Committee, 'Fighting Fraud: Breaking the Chain', 2022, p. 73, <https://committees.parliament.uk/publications/31584/documents/177260/default/>, accessed 12 June 2026.

87 Ofcom, 'Tackling Scam Calls: Updating Our CLI Guidance to Expect Providers to Block More Calls with Spoofed Numbers', 29 July 2024, <https://www.ofcom.org.uk/siteassets/resources/documents/consultations/category-2-6-weeks/276698---further-action-to-tackle--scam-calls/associated-documents/statement-tackling-scam-calls.pdf>, accessed 12 June 2026.

88 See, for example, the training programme 'Fundamentals of Fraud Combating', developed jointly by the central bank and a banking institution (Egypt): Central Bank of Egypt and Egyptian Banking Institute, 'Central Bank of Egypt and Egyptian Banking Institute Launch "Foundations of Fraud Combating" Training Program for Banking Sector Employees', press release, updated 28 December 2025, <https://www.cbe.org.eg/en/news-publications/news/2025/12/28/13/42/ebi-fraud-combating>, accessed 12 June 2026.

89 GIRAF is a global informal forum for telecom regulators. See GIRAF, One Consortium, <https://oneconsortium.org/giraf/>, accessed 29 June 2026.

90 GSM Association, 'Scams Content Hub', <https://www.gsma.com/solutions-and-impact/technologies/security/scams/scams-content-hub/>, accessed 29 June 2026; Benda, 'Fraud and Scams TF'.

91 International Justice Mission, 'Forced Scamming', <https://www.ijm.org/our-work/trafficking-slavery/forced-scamming>, accessed 12 June 2026.

92 Nettideittiturva, 'Romance Scam Recovery Project', <https://nettideittiturva.fi/info/in-english/>, accessed 12 June 2026.

93 IDCARE, 'National Identity & Cyber Support', <https://www.idcare.org/>, accessed 12 June 2026.

94 See also Interpol, 'INTERPOL Urges End to "Pig Butchering" Term, Cites Harm to Online Victims', press release, 17 December 2024, <https://www.interpol.int/en/News-and-Events/News/2024/INTERPOL-urges-end-to-Pig-Butchering-term-cites-harm-to-online-victims>, accessed 12 June 2026.

© Royal United Services Institute

95 Ministry of Home Affairs (Singapore), 'The Singapore Special Event "Beyond Borders: A Whole-of-Society Approach to Disrupting Scams Internationally" at the 2nd Global Fraud Summit – Opening Remarks by Mr Edwin Tong, Minister for Law and Second Minister for Home Affairs', 18 March 2026, <https://www.mha.gov.sg/media-room/newsroom/the-singapore-special-event-beyond-borders-a-whole-of-society-approach-to-disrupting-scams-internationally-at-the-2nd-global-fraud-summit/>, accessed 12 June 2026.

96 Anti-Deception Coordination Centre (Hong Kong), <https://www.adcc.gov.hk/en-hk/home.html>, accessed 12 June 2026.

97 Dass, 'The Anti-Scam Centre'.

98 National Scam Response Centre (Malaysia), 'About NSRC', <https://nfcc.jpm.gov.my/index.php/en/about-nsrc>, accessed 12 June 2026.

99 Otoritas Jasa Keuangan, 'The Rise of Scams: OJK and the Government Launch National Campaign to Combat Scam and Illegal Financial Activities', press release, 19 August 2025, <https://ojk.go.id/en/berita-dan-kegiatan/siaran-pers/Pages/The-Rise-of-Scams-OJK-and-the-Government-Launch-National-Campaign-to-Combat-Scam-and-Illegal-Financial-Activities.aspx>, accessed 12 June 2026.

100 See, for example, American Bankers Association, 'ABA Fraud Contact Directory', <https://www.aba.com/banking-topics/risk-management/fraud/directory>, accessed 12 June 2026.

101 Author interview, online, 12 December 2025.

102 One Consortium, 'International Traceback', <https://oneconsortium.org/international-traceback/>, accessed 12 June 2026.

103 Not public; however, interested national authorities are encouraged to obtain this document from Interpol.

© Royal United Services Institute

195 years of independent thinking on defence and security

The Royal United Services Institute (RUSI) is the world's oldest and the UK's leading defence and security think tank. Its mission is to inform, influence and enhance public debate on a safer and more stable world. RUSI is a research-led institute, producing independent, practical and innovative analysis to address today's complex challenges.

Since its foundation in 1831, RUSI has relied on its members to support its activities. Together with revenue from research, publications and conferences, RUSI has sustained its political independence for 195 years.

© The Royal United Services Institue for Defence and Security Studies

RUSI is registered as a charity in England and Wales

Charity number: 210639

VAT number: GB752275038