GSMA Intelligence

Strengthening digital trust in Asia Pacific: preventing scams through shared intelligence



© 2026 GSMA Intelligence

GSMA

The GSMA is a global organisation unifying the mobile ecosystem to discover, develop and deliver innovation foundational to positive business environments and societal change. Our vision is to unlock the full power of connectivity so that people, industry and society thrive. Representing mobile operators and organisations across the mobile ecosystem and adjacent industries, the GSMA delivers for its members across three broad pillars: Connectivity for Good, Industry Services and Solutions, and Outreach. This activity includes advancing policy, tackling today's biggest societal challenges, underpinning the technology and interoperability that make mobile work, and providing the world's largest platform to convene the mobile ecosystem at the MWC and M360 series of events.

We invite you to find out more at gsma.com

GSMA Intelligence

GSMA Intelligence is the definitive source of global mobile operator data, analysis and forecasts, and publisher of authoritative industry reports and research. Our data covers every operator group, network and MVNO in every country worldwide — from Afghanistan to Zimbabwe. It is the most accurate and complete set of industry metrics available, comprising tens of millions of individual data points, updated daily.

GSMA Intelligence is relied on by leading operators, vendors, regulators, financial institutions and third-party industry players, to support strategic decision-making and long-term investment planning. The data is used as an industry reference point and is frequently cited by the media and by the industry itself.

Our team of analysts and experts produce regular thought-leading research reports across a range of industry topics.

www.gsmaintelligence.com

info@gsmaintelligence.com

Author

Kenechi, Okeleke, Senior Director, GSMA Intellience

Contributors

Jeanette Whyte, Head of Policy & External Affairs, GSMA Asia Pacific

Ming Sheng Bensen Koh, Policy Director, GSMA Asia Pacific

Samuel Perks, Senior Policy Manager, GSMA Asia Pacific

We would also like to acknowledge the support of the GSMA Asia Pacific Cross-Sector Anti-Scam Taskforce (ACAST) to this report.

Contents

Executive summary 2

1. Building digital trust: a shared responsibility 3

1.1 The risks of fragmented responses 4

1.2 The shift towards a collaborative response 5

1.3 Data sharing as a tool for collective response 6

2. Building sustainable ecosystems for telecoms data sharing 7

2.1 The role of telecoms data in combating fraud and scams 7

2.2 Key factors for trusted and sustainable telecoms data sharing 8

3. The GSMA Data Exchange Proof of Concept 17

3.1 Overview and key features 17

3.2 Learnings from the pilot 19

4. Scaling up telecoms data sharing beyond pilots 23

4.1 Align stakeholders around shared incentives and a clear commercial vision 24

4.2 Drive a shift in organisational mindsets to support collaborative data sharing 25

4.3 Creating the enabling environment for data sharing 26

Executive summary

Fraud and scams have become one of the most significant threats to digital trust across Asia Pacific, fuelled by organised crime gangs adopting AI-powered phishing, deepfakes, social engineering and increasingly sophisticated cross-platform attack models.

As fraudsters simultaneously exploit legitimate infrastructure such as telecoms networks, digital platforms, financial services and other digital channels, traditional siloed approaches to detection and prevention are proving inadequate. No single organisation has complete visibility of the scam lifecycle, creating information gaps that fraudsters can exploit. As a result, scam prevention is increasingly being recognised as a shared responsibility that requires coordinated action by digital ecosystem participants.

Telecoms operators can play an important role within this ecosystem, especially because operators have direct contact with victims (though scams affect the entire digital ecosystem). Through access to network intelligence such as call records, SIM-swap activity, messaging patterns and device signals, operators often observe scam indicators earlier in the attack chain. When combined with intelligence from other ecosystem participants, telecoms signals can support earlier detection, improve risk assessment and enable more proactive intervention against scams. However, unlocking this value requires trusted, scalable and sustainable mechanisms for data sharing that address challenges around trust, interoperability, incentives, privacy and regulation.

The GSMA Data Exchange Proof of Concept provides valuable evidence that privacy-preserving telecoms data sharing is both feasible and effective. It highlights four critical foundations for sustainable ecosystem development: governance frameworks built on trust and accountability; privacy-preserving approaches that enable collaboration without exposing sensitive data; operational models focused on data quality, scale and timing; and commercial frameworks that reward prevention outcomes. Importantly, the commercial opportunity is not limited to data sharing itself. Telecoms signals can potentially be transformed into actionable risk intelligence, including indicators, scores and preventative capabilities that create value for participants while supporting earlier scam prevention. These learnings provide a blueprint for evolving telecoms data sharing from isolated pilots into trusted, ecosystem-wide scam-intelligence infrastructure.

Scaling up telecoms data sharing beyond pilots will require broader ecosystem participation. Specifically, this requires the following actions from ecosystem participants:

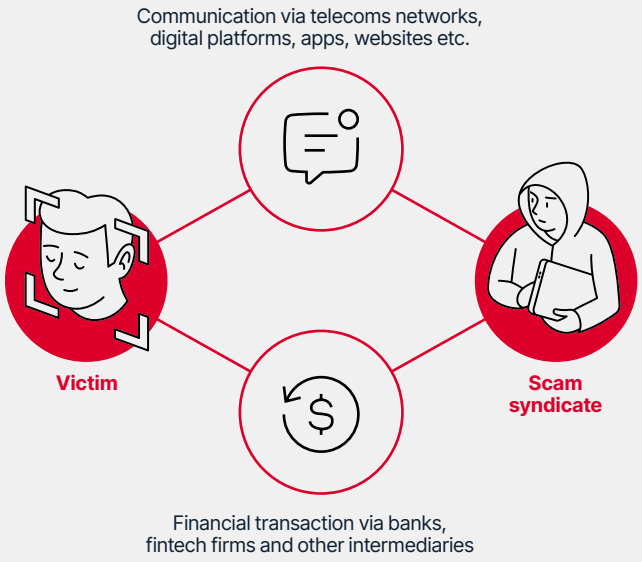
- **Align stakeholders around shared incentives and a clear commercial vision:** Stakeholders may use commercial models that focus on scam-prevention outcomes, recognise participant-level value and support collective ecosystem benefits. This may include models that create value from actionable scam-intelligence and preventative capabilities rather than simply monetising access to underlying data.
- **Drive a shift in organisational mindsets to support collaborative data sharing:** Data sharing could be positioned as a strategic priority, backed by executive sponsorship and enabled by multi-directional intelligence sharing.
- **Recognise the role of AI and API capabilities in the future data-sharing ecosystem:** These tools may be used to address emerging threats, while a roadmap could be developed, from batch-based sharing to API-enabled collaboration, that supports faster, scalable solutions.
- **Foster an enabling regulatory regime that facilitates appropriate data-sharing architecture to fight scams and fraud:** This includes safe-harbour provisions, consent mechanisms and data-sharing clarifications.

01.
Building digital trust: a shared responsibility

Digital trust has become a foundational requirement for inclusive digital transformation, economic growth and national resilience. Rapid technological advancements, particularly in AI, have also introduced new risks, including AI-powered cyberthreats, deepfakes, social engineering and automated tools for criminal exploitation. The 2025 Global State of Scams Report estimates that consumers across 42 countries lost approximately $442 billion to scams in the past year,[1] while the 2026 Interpol Global Financial Fraud Threat Assessment finds that AI-enhanced scams are 4.5× more profitable than traditional methods.[2] More broadly, the erosion of digital trust can undermine consumer confidence, discourage business investment and innovation, weaken trust in digital public services and ultimately hinder social and economic progress.

Scammers purposefully combine offline and online methods and vary modes of communications and payment. They also exploit a range of resources from the financial, telecoms and technology sectors as part of their operations. This is all in order to confuse victims and evade detection. Therefore, siloed defences are no longer sufficient in an increasingly sophisticated threat landscape. An effective responses requires a collaborative, intelligence-led approach that is aligned with the cross-sector nature of modern threats. Figure 1 illustrates a typical multi-channel scam scenario involving multiple actors across the digital ecosystem, highlighting that no single company or sector has a complete view of the scam operational chain. This fragmentation limits the ability of ecosystem players to detect and disrupt threats in a timely manner.

Figure 1 A typical multi-actor scam chain



Source: GSMA Intelligence

1 Global State of Scams Report 2025, Global Anti-Scam Alliance, 2025
2 Interpol Global Financial Fraud Threat Assessment, Interpol, 2024

This common scenario underscores the urgency for digital ecosystem players to address scams as a shared responsibility. This is critical to protecting vulnerable users, supporting economic stability and sustaining trust in the digital economy. By combining cross-sector insights with advanced analytics, organisations can strengthen their collective defences, creating a network effect that enables faster and more effective responses to scams while enhancing detection capabilities across the ecosystem.

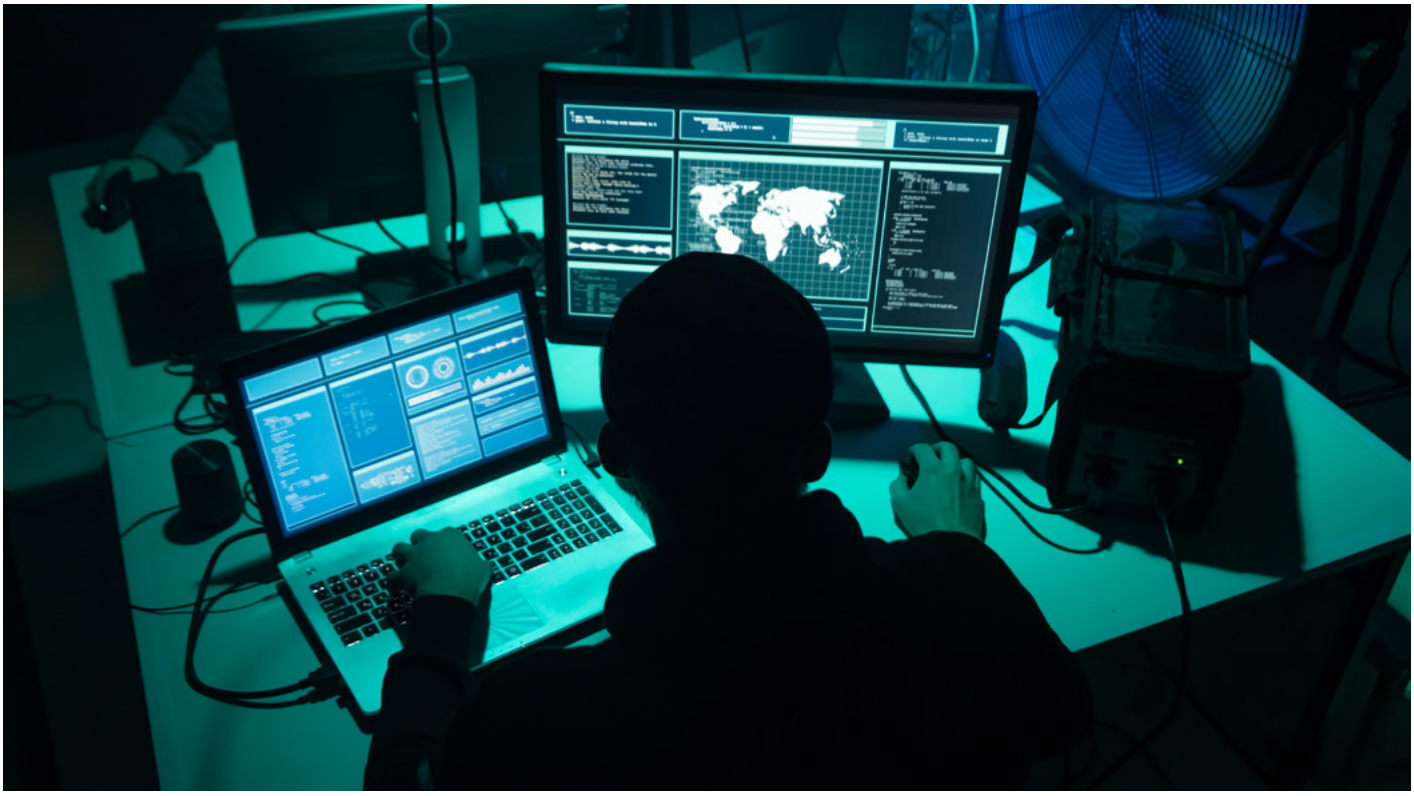
For example, telecoms operators can block known scam callers or suspicious SIMs flagged by banks or digital platforms; banks can identify or freeze transactions linked to accounts reported as fraudulent by operators or e-commerce providers; social media platforms can remove scam accounts traced through phone numbers or payment details; and regulators and law enforcement can use a cross-sector view to inform and coordinate policy and enforcement action.

1.1 The risks of fragmented responses

Fragmented and ineffective responses to tackling fraud and scams carry substantial and multifaceted risks for digital ecosystem participants. At a fundamental level, victims face significant emotional and psychological harm, while enterprises risk operational disruption, reputational damage and considerable financial losses. These impacts also have broader implications for growth and innovation across the digital ecosystem:

- **Erosion of digital trust**: When users lose confidence in the ability of digital ecosystem players to protect them, they may reduce engagement with online services, hesitate to adopt digital payments and other services, or even abandon digital platforms altogether. The same applies on the enterprise side, where businesses may delay digital transformation and AI adoption due to concerns over cybersecurity, regulatory uncertainty and compliance risks. Ultimately, declining digital trust weakens customer loyalty, erodes brand equity and constrains long-term revenue growth across the digital ecosystem.
- **Reactive rather than proactive responses**: Siloed defences allow scammers to exploit information gaps, leaving organisations trapped in a reactive cycle and unable to pre-empt or disrupt attacks before they occur.
- **Prescriptive and fragmented regulation**: Growing concerns and evolving expectations around online trust are prompting some governments to consider increasingly prescriptive and reactive regulatory measures. While well intentioned, these measures can be difficult to enforce in practice. A coordinated, evidence-based approach, supported by strong collaboration between governments and industry, is essential to restore trust.
- **Shared liability and reimbursement**: Governments are increasingly introducing frameworks that require multiple sectors to share financial responsibility for consumer losses that arise from online harms. These approaches aim to strengthen consumer protection, but inconsistent and, in some cases, counterproductive liability models across jurisdictions risk creating regulatory fragmentation, increasing compliance costs and weakening incentives for cross-sector collaboration.

These risks translate into rising compliance costs, regulatory fines and remediation efforts, which may ultimately exceed the upfront investment required for more collaborative approaches. In addition, stricter controls may inadvertently push users towards unregulated channels, where exposure to fraud and cyberthreats is often greater.



1.2 The shift towards a collaborative response

Historically, telecoms operators, digital platforms and financial institutions across Asia Pacific have worked largely in silos, constrained by fragmented cross-border regulation. Cybercrime responses have typically been reactive, with each sector managing threat detection internally rather than sharing intelligence through trusted, open channels. However, there is growing recognition of the need for a coordinated response to fraud and scams.

At the GSMA Asia Pacific CEO and CRO Digital Leaders' Summit in March 2026, participants agreed that collaboration is essential to building trust and preventing scams at scale, and that deeper ecosystem coordination could further strengthen prevention efforts. This view is shared widely across the ecosystem, as reflected in the growing number of initiatives in recent years aimed at facilitating cross-sector collaboration.

The GSMA-led Asia Pacific Cross-Sector Anti-Scam Taskforce (ACAST) is a leading example. Launched in June 2025 as part of the GSMA's United Against Scams initiative, ACAST brings together telecoms operators, digital platforms, technology specialists and public authorities to coordinate evidence, share threat intelligence, align technical approaches and explore privacy-respecting data-sharing models to combat fraud and scams.

As the region's first structured cross-sector mechanism designed to address scams, ACAST provides a strong foundation for collaborative action. It supports a shift away from working in silos towards a more unified response to cybercrime, addressing the fragmentation that fraudsters exploit. By enabling essential information exchange and coordinated intervention, it strengthens the ability to detect, block and disrupt threats through network-level controls, spam monitoring and other detection techniques. As of March 2026, ACAST had 39 members from 17 countries.[3]

Several other initiatives have also emerged with a more global focus. The Global Signal Exchange (GSE) – which was launched by the Global Anti-Scam Alliance, the DNS Research Federation and Google – is designed as an internet-scale clearinghouse for scam and fraud signals, enabling trusted participants to share and access abuse data more efficiently. Another example is Meta's ThreatExchange, an API-supported platform and open-source toolkit that helps security, trust and safety teams exchange threat signals, malware data, phishing indicators and bad-actor telemetry in near real time.

3 "The scam economy thrives in silos. Coordination is our strongest defence", GSMA, March 2026

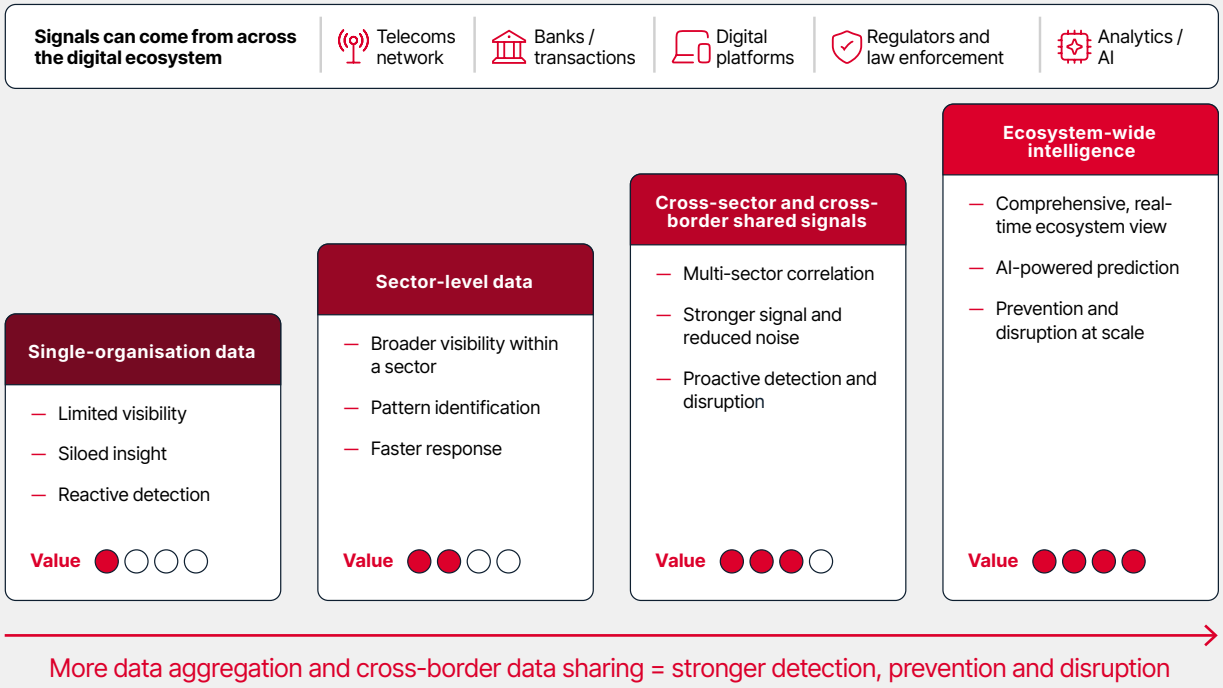
1.3 Data sharing as a tool for collective response

Digital ecosystem participants possess vast amounts of distinct datasets. For example, telecoms operators have access to call data records, SIM-swap events and network signalling data, providing unique visibility into the origin and flow of communications across networks. Meanwhile, digital platforms capture account creation patterns, user interactions and behavioural signals, helping identify how users are targeted and groomed online. And financial institutions hold transaction records and device footprints, enabling them to track money flows and app access patterns.

Unlike physical assets, data's value does not come from exclusive ownership. Instead, its value grows when it is combined with other sources of data. No organisation has a complete view of digital threats, as each dataset offers only a partial perspective. Responsible cross-sector data sharing can connect isolated data sets and reveal wider patterns of malicious activity.

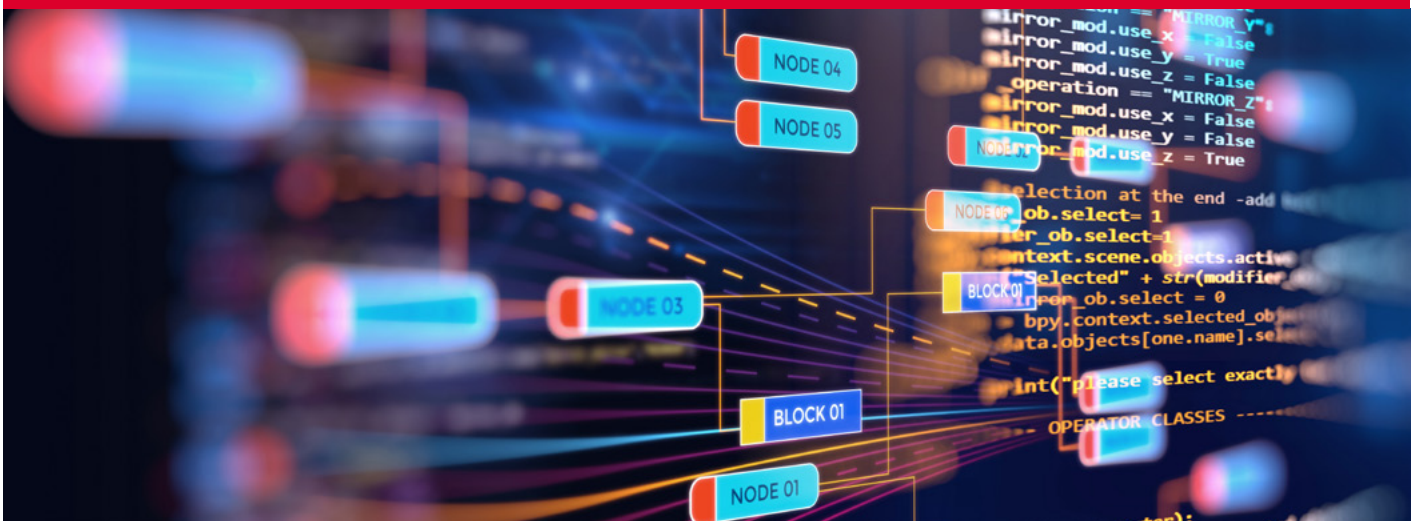
Figure 2 illustrates how data value exists on a spectrum, increasing with each layer of aggregation – from isolated, organisation-level insights to ecosystem-wide intelligence.

Figure 2 Data value increases with aggregation



Source: GSMA Intelligence

For digital ecosystem participants, this means that moving from fragmented, siloed interventions to a coordinated, collective response depends on aggregating relevant datasets (or 'signals') through sustainable and privacy-respecting data-sharing mechanisms to enhance detection, prevention and mitigation outcomes.



02
Building sustainable ecosystems for telecoms data sharing

2.1 The role of telecoms data in combating fraud and scams

With more than 2.6 billion connections across Asia Pacific, mobile networks are a key entry point and coordination layer that is being exploited for scam activities, including phishing, scam calls, social engineering and the recruitment of money mules. This gives telecoms operators an important vantage point in combating scams, as they can leverage, where legally permitted and appropriate, network data – such as call records, SMS patterns, device identifiers (e.g. IMEI), geolocation signals and communication graphs – to identify high-value risk indicators, including SIM swaps, suspicious calling activity and anomalous messaging patterns.

These signals, which are largely invisible to other digital ecosystem participants operating in isolation, often provide an early warning of fraudulent activity. This upstream visibility makes telecoms data one of the most valuable – yet underutilised – assets in the fight against scams.

The value of telecoms signals extends across the wider digital ecosystem. Banks and payment providers can use these signals to strengthen pre-transaction risk assessments and reduce account takeover fraud. Meanwhile, social media platforms and e-commerce providers can use these signals to verify users, detect malicious accounts and adverts, identify location spoofing and disrupt phishing, vishing and other social engineering campaigns closer to the source. More broadly, aggregating telecoms signals with financial, identity and digital platform data can create a richer cross-sector view of risk, helping to uncover fraud networks, improve detection accuracy and reduce false positives.

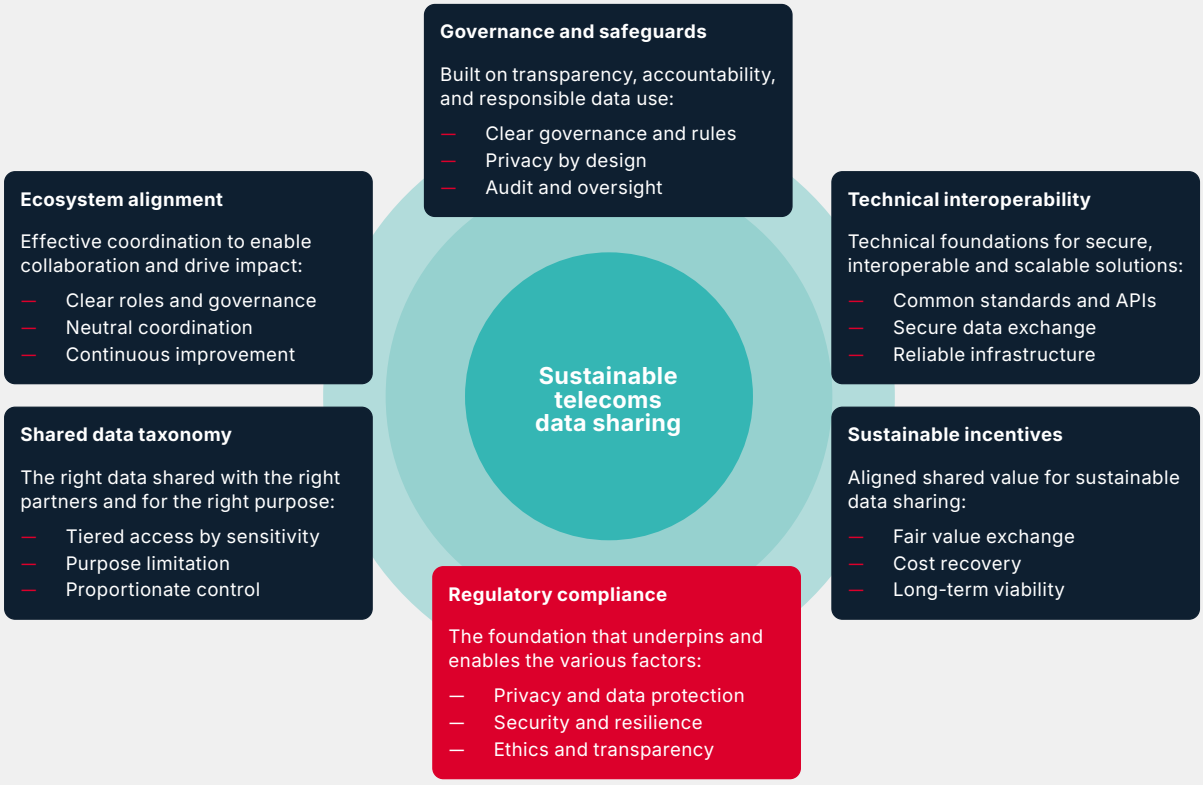
In practical terms, telecoms data can help shift the digital ecosystem from reactive response to proactive prevention. This is particularly important in Asia Pacific, where fraud and scam activity remains high and policymakers are increasingly adopting cross-sector approaches to consumer protection. By enabling earlier detection of suspicious activity and supporting more coordinated interventions, telecoms data can play a critical role in strengthening ecosystem-wide fraud-prevention efforts.

Despite growing recognition of the value of telecoms data in combating scams, most data-sharing initiatives remain limited in scale and impact. Fragmented bilateral partnerships, inconsistent standards, regulatory uncertainty, high integration costs and misaligned incentives continue to hinder ecosystem-wide collaboration. The challenge is no longer proving the value of telecoms data but establishing trusted and sustainable mechanisms for its secure and continuous exchange. Unlocking the full potential of telecoms signals may require scalable data-sharing frameworks, common standards and stronger cross-sector collaboration.

2.2 Key factors for trusted and sustainable telecoms data sharing

Unlocking the value of telecoms data for scam prevention depends on a set of foundational enablers that make data sharing not only possible, but also trusted, scalable and sustainable. Figure 3 highlights five critical factors needed to create the conditions for secure and effective collaboration, underpinned by enabling regulatory and policy frameworks. These factors can help realise the full value of telecoms data, allowing it to play a greater role in proactive fraud prevention across the digital ecosystem.

Figure 3 Key factors for sustainable telecoms data sharing



Source: GSMA Intelligence

2.2.1 Governance and safeguards

A sustainable telecoms data-sharing ecosystem depends on effective governance and robust safeguards. Almost 75% of consumers in countries in the Association of Southeast Asian Nations (ASEAN) are willing to have mobile operators share their personal data if it helps combat scams, provided appropriate safeguards are in place, according to the GSMA ASEAN Consumer Survey Report 2025. This highlights that consumers recognise the value of responsible data sharing and are generally willing to share data when the benefits are clear. In contrast, comfort with conversational-app data sharing has dropped from 53% to 40%, reflecting concerns about impersonation and phishing on those platforms.

The challenge is to balance the protection of consumer privacy with the need to enable responsible data sharing that strengthens digital trust and safety. Striking this balance will become increasingly important as digital harms continue to evolve and issues such as online safety become more prominent.

For organisations, strong governance is a prerequisite for participation. Telecoms operators, banks, digital platforms and other ecosystem participants will only share valuable signals if they are confident that data will be handled securely, used only for agreed purposes and protected from misuse. Without this confidence, data sharing is likely to remain confined to fragmented initiatives that struggle to achieve ecosystem-wide impact. Building trust requires clear governance, accountability and transparency, supported by well-defined rules on what data can be shared, who can access it, how it can be used and how compliance will be monitored.

Technology and operational safeguards have an important role to play. Privacy-enhancing technologies, role-based access controls, audit trails and data-minimisation principles can help ensure sensitive information is handled responsibly. These measures should be complemented by clear legal agreements and operating procedures that establish accountability and provide mechanisms for resolving disputes when issues arise.

Several initiatives demonstrate the value of strong governance and safeguards. Singapore's anti-scam ecosystem brings together telecoms operators, financial institutions and government agencies under shared governance arrangements to combat scams more effectively. Similarly, Stop Scams UK has established a framework that enables telecoms, banking and technology companies to exchange threat intelligence while maintaining appropriate safeguards.

2.2.2 Technical interoperability

Even when organisations are willing to collaborate, data sharing cannot scale up without common technical standards and supporting infrastructure. Many existing initiatives rely on bespoke integrations between individual organisations, creating complexity, high implementation costs and limited interoperability. While such an approach may be effective for specific use cases, they become increasingly difficult to manage as additional participants join the ecosystem. Interoperability is therefore important to allow telecoms operators, financial institutions, digital platforms and law enforcement agencies to exchange data seamlessly despite diverse legacy systems, technologies and vendor environments. This includes agreeing on common or interoperable taxonomies, so that various terms in the scams and fraud lexicon are commonly understood and corresponding data can be easily exchanged between different actors.

Standardisation also reduces friction, improves data quality and consistency and enables information to be exchanged efficiently. Common data models, interoperable APIs, identity frameworks and security standards can allow participants to connect once and collaborate with many partners. This lowers implementation costs and improves the reliability of shared intelligence. Timely exchange is particularly important in fraud prevention, where many risk signals have a short operational lifespan and delays can significantly reduce their effectiveness.

Emerging industry initiatives demonstrate how common standards can help overcome these challenges. The GSMA Open Gateway and CAMARA APIs provide a framework for exposing telecoms network capabilities through standardised interfaces. APIs relating to number verification, SIM swap, device location, device intelligence and scam signals can enable other ecosystem participants to access trusted telecoms signals in a timely, consistent and scalable manner.

2.2.3 Sustainable incentives

A lack of sustainable incentives can undermine data-sharing initiatives, limit participation and ultimately prevent them from achieving scale and long-term impact. While the public benefits of data sharing are clear – including reduced fraud losses, stronger digital trust and a more resilient digital ecosystem – telecoms operators incur significant costs for data collection, processing, infrastructure, compliance and operational management. Without incentives that align costs and benefits across participants, there is a risk that data sharing will remain confined to pilots, isolated partnerships or regulatory mandates, leaving gaps that sophisticated fraud networks can exploit.

Creating sustainable data-sharing ecosystems therefore requires commercial models that align incentives, distribute costs fairly, create mutual and comparable value for participants, spark tangible action and encourage long-term commitment. These can help drive the required investment in data quality, technical capabilities and operational processes to transform data sharing from a compliance obligation into a strategic capability.

Importantly, incentive models should recognise and reward organisations that contribute high-quality signals while ensuring they can recover the costs associated with data collection, processing and sharing. At the same time, sustainable data sharing should not be driven primarily by monetising access to information. There is, however, an important distinction between monetising access to underlying data and creating commercial value from derived intelligence, such as risk indicators, scores or insights that enable fraud prevention. Existing commercial fraud and threat intelligence services demonstrate that actionable intelligence can form the basis of a sustainable risk-prevention proposition without requiring customers to access the underlying datasets.

More broadly, incentive structures should be designed to reward outcomes, aligning participants around the shared objective of reducing fraud and scams across the ecosystem. This not only strengthens the effectiveness of data-sharing initiatives but also helps preserve trust in the digital services and platforms that consumers and businesses increasingly depend on.

A variety of commercial models have emerged to support sustainable telecoms data sharing, each with different implications for participation, scalability and long-term viability. Table 1 assesses the principal approaches and the trade-offs associated with each, highlighting their relative strengths and limitations in enabling the large-scale exchange of telecoms signals to combat fraud and scams.

Table 1: Examples of commercial models for data-sharing initiatives

Model	Description	Benefits	Limitations
Per-query fee	Participants pay for each data access or risk-check request	Easy to implement and ties fees directly to usage	Creates friction at the point of use, discourages frequent checks, rewards volume over impact and may exclude smaller participants
Subscription	Participants pay a fixed fee for access during a set period	Provides predictable costs for participants, stable funding for the initiative and stronger incentives to use shared intelligence	Monetises access rather than impact and does not directly reward contributors that provide the most valuable signals
Tiered subscription	Participants pay tiered fees based on size, transaction volume, fraud exposure or intelligence needs	More equitable than a flat subscription, easier to procure and budget for and widely used in data and intelligence services	Monetises access rather than impact and high-value contributors may pay the same as those receiving the greatest benefit, providing limited incentives to improve intelligence quality
Contribution-based access	Participants earn discounts, credits or enhanced capabilities based on the quality and volume of signals they contribute	Encourages active participation, addresses free-rider problems and incentivises contributions of new intelligence	Contribution value can be difficult to measure and, if poorly designed, may encourage quantity over quality
Cooperative funding	Participants fund shared infrastructure through membership contributions, treating it as an industry utility rather than a commercial data service	Builds trust, encourages broad ecosystem participation and prioritises collective outcomes over commercial monetisation	May weaken commercial incentives for rapid innovation and create more complex governance requirements
Insurance funded	Fraud insurers or risk underwriters fund initiatives to support the ecosystem	Strongly linked to risk reduction and creates an additional funding source	Requires a mature ecosystem and makes causality difficult to attribute
Government funding	Government funding to support participation in fraud prevention platforms	Speeds up ecosystem development, lowers participation barriers, supports public interest goals and enables smaller firms to participate	Can create reliance on public funding, reduce efficiency incentives, increase political influence and weaken long-term sustainability
Outcome-based models	Participants pay based on the value generated	Aligns incentives with fraud reduction, rewards value creation over data consumption and strengthens the business case for participation	More complex to implement because outcomes can involve multiple participants, attribution is difficult and benefits may take time to materialise

Source: GSMA Intelligence

A key takeaway from the assessment of these models is that the most sustainable long-term models are likely to be shared-value or outcome-based frameworks that align commercial incentives with fraud-prevention results. Rather than charging for access alone, these models reward measurable impact, such as fraud losses prevented, funds recovered and criminal accounts disrupted. They may also include models in which participating organisations transform underlying signals into actionable risk intelligence or preventative capabilities, creating commercial value from the intelligence generated rather than from access to the underlying data itself. These could take several forms:

- **Fraud-loss-reduction sharing**: Participants contribute a share of verified scam losses prevented.
- **Success-based intelligence rewards**: Data contributors are compensated when their signals directly support fraud detection or disruption.
- **Hybrid membership models**: Fixed participation fees fund shared infrastructure, with additional payments linked to measurable outcomes.
- **Ecosystem utility models**: Participants fund a shared platform based on their exposure to fraud risk, such as transaction volume or customer base.
- **Intelligence-as-a-service models**: Participants pay for actionable risk intelligence, scores or preventative capabilities derived from multiple signals, rather than for access to the underlying datasets.

Indirect incentives can also support participation, including liability protections for good-faith data sharing (also known as 'safe harbour' and 'Good Samaritan' protections), stronger consumer trust and opportunities to develop value-added scam prevention services with banks, fintechs and digital platforms. India's Digital Intelligence Platform,[4] for example, links telecoms data-sharing contributions to measurable outcomes such as frozen mule accounts and prevented financial losses.

2.2.4 Shared data taxonomy and graduated threat classification

In the fight against scams, effective data sharing is not a binary choice between openness and secrecy. Not all data carries the same level of sensitivity, nor should all stakeholders have access to the same information. A tiered data-sharing architecture provides a framework for balancing impact, privacy, legal compliance and trust by classifying intelligence according to its characteristics.

Scam intelligence spans a broad range of data, from public web artefacts to highly sensitive banking records. It can be assessed against two core dimensions:

- **Data risk and impact:** This reflects the potential harm to individuals or businesses if data is leaked or misused. Low-impact data, such as anonymised technical indicators or public web artefacts, can be shared with limited friction. High-impact data, including sensitive personal information, victim records or live user telemetry, requires strong governance, encrypted access and strict safeguards to prevent secondary harm or regulatory breaches.
- **Signal verifiability and maturity:** Threat intelligence also varies by confidence level. A single user report may be noisy and should mainly support awareness. As additional signals corroborate it, confidence increases, enabling stronger interventions. This allows participants to scale their response proportionately, reserving actions such as account freezes for high-confidence intelligence.

Table 2 applies these dimensions in a four-quadrant matrix, providing an illustrative framework for categorising scam signals ('light grey' denotes data with low sensitivity, while 'deep black' denotes high sensitivity). Although implementation will require greater technical detail, the matrix offers a clear baseline for matching different types of threat intelligence with suitable sharing protocols.

4 Digital Payments Intelligence Platform, Reserve Bank Innovation Hub, 2026

Table 2: Threat intelligence matrix by risk and verifiability

	Light grey (low sensitivity)	Deep black (high sensitivity)
High risk	**Privacy-preserved signal sharing and secure evaluation:** This includes real-time behavioural anomalies and isolated, unverified signals, such as a live phone call during a banking transaction, sudden changes in device-use patterns or a single user complaint. Given the high risk of false positives, these signals should be securely assessed across sectors to corroborate indicators and increase confidence before being treated as confirmed malicious activity.	**Restricted and regulated sharing:** This includes legally verified evidence and sensitive records, such as confirmed mule SIMs, bank-verified mule accounts, victim financial records and court-ordered asset freezes. Given the high privacy impact and strict legal requirements, these signals should be shared securely and directly with authorised stakeholders and law enforcement under statutory safeguards.
Low risk	**Open dissemination:** This includes publicly available or unverified indicators, such as scam URLs, deceptive ad screenshots or user-flagged public posts. Because these signals may carry relatively low risk, subject to case-by-case assessment and validation, they can be shared through open feeds and public portals to raise immediate ecosystem awareness and support further validation towards 'deep black' status, with appropriate safeguards against misuse and mechanisms for correction.	**Automated exchange:** This includes technical infrastructure footprints and deterministic network indicators, such as malicious IP addresses, confirmed scam numbers and expired or recycled MSISDNs. Their high confidence and potentially low privacy impact may support real-time, machine-to-machine exchange across sectors for automated threat mitigation, subject to verification, freshness, proportionality, appropriate access controls and prompt correction or appeal mechanisms.

Source: GSMA Intelligence

The matrix shows that scam intelligence is not uniform. Data varies by sensitivity, quality, accuracy and operational value, so different sharing mechanisms are required. Low-risk, high-confidence technical indicators are suitable for rapid automated exchange, while low-risk, low-confidence signals are better shared through open dissemination, allowing the wider ecosystem to validate, enrich and develop them into more reliable intelligence.

Meanwhile, high-risk, low-confidence signals require more careful handling. Privacy-preserved cross evaluation enables organisations to compare indicators without exposing sensitive data, helping corroborate suspicious activity and reduce false positives. Once intelligence reaches a high confidence level and the relevant legal thresholds are met, restricted and regulated sharing allows sensitive information to be exchanged under clear governance arrangements, statutory authority and access controls.

By matching each sharing mechanism to the data's sensitivity, quality and accuracy level, the framework ensures that the right information reaches the right participants at the right time, strengthening threat detection while protecting privacy, security and applicable legal requirements. Crucially, this tiered architecture should be seen not as a compliance burden but as a strategic enabler of proactive scam prevention. Combined with common standards and privacy-preserving mechanisms,[5] it can turn isolated data points into actionable cross-sector intelligence, supporting real-time detection, faster network disruption and a more resilient digital ecosystem.

5 Technical and governance measures, such as encryption, anonymisation and secure data-sharing environments, that allow data to be used or shared while protecting sensitive personal information.



2.2.5 Ecosystem alignment

Unlike fragmented bilateral agreements, cross-sector scam prevention relies on ecosystem coordination to align multiple digital ecosystem participants around shared standards, governance frameworks and interoperable rules of engagement needed to align diverse market participants. Without such coordination, organisations will focus on their own risks and priorities, creating gaps in visibility and fragmented defences that cross-border scam networks easily exploit.

Crucially, effective coordination does not require a single, centralised state orchestrator or monolithic data hub.[6] Instead, modern anti-scam architectures can succeed through a federated model, combining sector-specific aggregation with decentralised cross-sector exchange. This allows competing participants to work together on shared challenges while maintaining commercial independence. Such coordination is particularly important in Asia Pacific, where regulatory frameworks, market structures and levels of digital maturity vary considerably and where scam networks increasingly operate across borders.

Asia Pacific's telecoms landscape is highly fragmented, with many markets served by numerous major operators and regional providers. This complexity makes sector-level alignment essential. Expecting banks, digital platforms, or government entities to build, manage and govern hundreds of bilateral integration points across this fragmented base is neither commercially nor operationally viable. Consolidating the telecoms layer within a common framework, for interaction purposes, would allow other sectors to access standardised interfaces, reducing integration friction, simplifying commercial agreements and preserving clear privacy boundaries.

At the national level, public authorities and anti-scam centres remain essential for setting regulatory floors, legal baselines and statutory safeguards. However, while state institutions are critical for enforcement and governance, a federated, multi-party exchange architecture is better suited to sharing different types of scam signals. Rather than relying on a single government node to route raw data, telecoms operators, financial institutions and digital platforms can exchange operational signals directly or through decentralised networks governed based on shared trust frameworks.

This federated model is particularly important for sensitive or probabilistic signals, such as live telemetry or behavioural anomalies, where false-positive risks are high. By analysing raw data locally in secure environments, organisations can correlate indicators and share high-confidence risk scores through decentralised networks without exposing raw subscriber personal data.

6 A central platform that enables users to discover, access and share datasets from multiple sources through a single point of access.

2.2.6 Regulatory compliance

Outcome- and evidence-based policy and regulatory frameworks provide the certainty to support sustainable data sharing. They define permissible use cases, establish accountability mechanisms and protect organisations that participate responsibly. Without explicit permissions or safeguards, telecoms operators and other ecosystem participants are likely to default to caution due to privacy and security obligations, data-sovereignty requirements and liability concerns.

Effective and holistic regulatory frameworks are a core enabler of telecoms data sharing. They should balance consumer protection, public-interest outcomes and innovation while creating the legal certainty needed for trusted, secure and scalable information exchange. Privacy and data protection remain essential, but sustainable telecoms data sharing also requires a broader regulatory framework that supports collaboration, responsible innovation and harm prevention. Regulation should therefore focus not only on whether data can be shared but also on the conditions under which it should be shared and the safeguards needed to ensure responsible use.

Policy and regulatory guidance can help achieve this balance:

- **Consent exemptions**: There are several types of consent exemptions, including scam prevention, crime prevention, public interest, legitimate interest, national interest and legal-obligation provisions. While each serves a different purpose, they share a common objective: enabling organisations to manage risks or fulfil broader societal obligations where obtaining consent would be impractical or would undermine the effectiveness of the activity.

  In the context of scam prevention, consent exemptions can provide an important legal basis for sharing data without explicit consent where there is a legitimate public-interest objective. Such provisions can reduce operational friction and support more proactive risk sharing, provided appropriate governance, privacy and security safeguards remain in place.

  For example, scam- and crime-prevention exemptions may enable the sharing of intelligence on suspected scams, mule accounts and malicious phone numbers, while public-interest provisions recognise that preventing scams delivers wider benefits for consumers, businesses and society.

  In Singapore, for instance, the Cosmic platform, which was introduced in 2023, allows financial institutions to share customer information on suspicious accounts without breaching standard confidentiality obligations. In the Philippines, Globe and GoTyme Bank signed a data-sharing agreement in February 2025 to strengthen fraud detection and investigation efforts by enabling the secure exchange of information on mobile numbers and accounts suspected of being linked to fraudulent activities. By allowing the two organisations to share relevant customer information – in compliance with the Philippines' Data Privacy Act and regulatory guidance from the Bangko Sentral ng Pilipinas and the National Privacy Commission – the agreement aims to accelerate investigations that would otherwise require lengthy legal processes. In India, the Digital Personal Data Protection Act 2023 carves out an exemption that allows entities to forgo consent requirements where personal data is processed in the interest of prevention, detection, investigation or prosecution of any offence or contravention of any law for the time being in force in India.

- **Safe-harbour provisions**: Legal uncertainty remains a major barrier to data sharing. Safe-harbour provisions can reduce this risk by protecting organisations that share scam-intelligence in good faith, follow approved governance frameworks and apply appropriate security and privacy controls. While many countries provide protections for reporting to law enforcement, explicit safe-harbour protections for voluntary cross-sector scam-intelligence sharing remain uncommon, highlighting an opportunity to expand this concept.

- **Regulatory sandboxes**: Regulatory sandboxes allow organisations to trial new data-sharing models, technologies and governance approaches under supervisory oversight. They allow policymakers to assess risks and benefits before introducing permanent rules while supporting responsible innovation in scam prevention. In Australia, the Enhanced Regulatory Sandbox, overseen by ASIC, allows eligible financial sector firms to test data-driven scam and identity solutions with real consumers for up to 24 months without holding a full Australian financial services licence or Australian credit licence.

- **Tiered data-sharing frameworks:** Tiered frameworks enable low-risk information, such as scam domains and aggregated trends, to be shared more widely while allowing stronger controls to be applied to personal data and high-confidence scam-intelligence. This proportionate approach maximises utility while managing privacy risk. India's Digital Intelligence Platform, for example, supports tiered, cross-sector intelligence sharing among more than 1,400 authorised participants, including telecoms operators, financial institutions and police, to help identify and disrupt scams.[7]
- **Industry codes, standards and certification:** Recognised codes of conduct, technical standards and certification schemes can set common rules for data quality, retention, security, auditability and access controls. This reduces uncertainty, improves interoperability and builds confidence among participants. Anti-phishing, anti-spam and know-your-customer frameworks often rely on industry-developed standards to define how information should be exchanged.
- **Competition law and antitrust guidance**: Clear competition law guidance and protocols can give organisations the confidence to collaborate on scam prevention. By defining what information can be shared and under what conditions, operators can engage in the collaboration which is necessary without fear of potential antitrust concerns.
- **Cross-border data transfer mechanisms**: Scams are inherently cross border, whereas regulation is often national. Mutual recognition agreements, harmonised regional frameworks, adequacy decisions and trusted transfer mechanisms can enable international data sharing and strengthen cross-border scam prevention. ASEAN is moving from policy declarations to operational collaboration by developing standardised intelligence-sharing mechanisms, common scam indicators and aligned reporting channels across member states. For example, the ASEAN Guide on Anti-Scam Policies and Best Practices, endorsed at the ASEAN Digital Ministers' Meeting in January 2026, provides regional guidance for governments and telecoms operators on sharing intelligence and mitigating scam calls and SMS.

In addition to these tools, which provide the legal certainty, trust and governance foundations needed to move telecoms data sharing towards sustainable, ecosystem-wide collaboration, regulatory parity across sectors is also important. Telecoms operators are often subject to stricter confidentiality and communications privacy obligations than other participants in the digital ecosystem, despite holding some of the most valuable scam signals. Greater regulatory alignment across telecoms, financial services and digital platforms can help ensure that these signals can be shared responsibly while maintaining equivalent standards of privacy, security and accountability across sectors.

7 "DoT and SEBI Sign MoU to Strengthen Fight Against Telecom-Linked Financial Frauds", Ministry of Communications, April 2026



03
The GSMA Data Exchange Proof of Concept

3.1 Overview and key features

Launched in 2025, the GSMA Data Exchange Proof of Concept (PoC) is an industry-led initiative that aims to establish a privacy-preserving framework for sharing scam-related signals with non-telecoms stakeholders. The project places particular emphasis on identifying upstream indicators of scam risk before a scam has been fully confirmed, enabling a more preventative approach to scam detection. Through the secure exchange and analysis of telecoms-derived scam signals, the PoC also seeks to identify which telecoms signals generate measurable scam-prevention outcomes and what type of data-sharing architecture would be most effective for large-scale deployment.

The PoC also shows the value of collaborative intelligence sharing by allowing participating telecoms operators to compare pseudonymised scam signals and identify both shared and unique indicators of scam activity. Aggregate analysis of de-identified data enables participants to assess overlaps in known fraudulent numbers, detect previously unseen threats and measure the additional value created through collaboration. In this way, the initiative tests the technical, operational and governance foundations needed for a broader telecoms-led scam-intelligence ecosystem.

The key features of the PoC are outlined below:

- **Demonstrates the value of collaborative scam prevention**: The PoC identifies both mutual matches (numbers flagged by multiple participants) and incremental matches (numbers identified by a single participant), helping quantify the additional intelligence generated through collective action compared to standalone scam detection.
- **Preserves privacy while enabling data sharing**: The PoC adopts a privacy-by-design approach, with telecoms numbers pseudonymised through key-based hashing before any data leaves a participant's environment. Only protected data and aggregated outputs are shared, reducing privacy, regulatory and reputational risks.
- **Provides a secure and scalable collaboration framework:** The initiative establishes common governance arrangements, data-protection mechanisms,[8] operational processes and analytical workflows that can support future expansion into larger and more sophisticated data-sharing ecosystems.

8 Technical and governance safeguards, such as encryption, access controls and secure data-sharing arrangements, designed to protect sensitive information and ensure compliance with privacy and data-protection requirements.

- **Generates actionable cross-operator intelligence**: By comparing scam signals across multiple telecoms operators, participants can identify suspicious numbers, scam typologies and risk indicators that may not be visible within a single network, strengthening the detection and understanding of scam activity.
- **Builds trust through a phased approach**: The PoC begins with aggregate analysis before progressing to bilateral and multilateral collaboration, allowing participants to build confidence in the legal, technical and operational model before moving towards more advanced intelligence sharing.
- **Supports the standardisation of scam signals and classifications**: Participants work to align scam categories, data definitions and analytical methodologies, helping establish a common language for cross-industry scam-intelligence sharing.
- **Provides evidence for future commercialisation**: The PoC is designed to demonstrate measurable value from shared scam-intelligence, creating a foundation for commercial models that incentivise data contribution and support sustainable ecosystem participation.
- **Creates a pathway to cross-industry collaboration**: While the initial focus is on telecoms operators, the target architecture envisages participation from banks, digital platforms and other ecosystem stakeholders, enabling richer intelligence sharing, enhanced scam detection and more effective scam prevention outcomes.

While the PoC offers significant potential, it also highlights several challenges that must be addressed to build a sustainable data-sharing ecosystem. Beyond technical and legal complexity, organisational friction remains a major barrier: although executive leaders often express strong support, operational progress can stall at middle-management level during legal, compliance and business-approval processes.

Other key challenges include inconsistencies in scam classification methodologies, varying levels of data maturity across operators, legal and regulatory uncertainty and the need to demonstrate clear value to participants. Addressing these issues will be critical to scaling up the initiative beyond the pilot phase and establishing a trusted, effective and commercially sustainable model for scam-intelligence sharing.

Nevertheless, the PoC represents an important step towards building the collaborative infrastructure required to combat scams at the ecosystem level. By testing mechanisms for secure data sharing, common governance and collective intelligence generation, it provides valuable insights into how telecoms operators and other stakeholders can collaborate more effectively to improve scam detection, strengthen consumer protection and lay the foundations for a more resilient digital economy.

How the GSMA Data Exchange PoC differs from other data-sharing initiatives

A key feature of the PoC is its emphasis on privacy-preserving collaboration. Rather than focusing solely on information sharing, the initiative explores technical approaches that allow multiple organisations to generate value from their data while minimising the exposure of underlying datasets. Participating organisations are expected to evaluate the effectiveness of different telecoms signals and determine which provide the greatest value in supporting scam-prevention activities.

This distinguishes the PoC from many existing data-sharing initiatives, which typically focus on exchanging information about known or confirmed bad actors. While platforms such as the GSE and Meta's ThreatExchange are primarily designed to facilitate the sharing of threat intelligence, the GSMA Data Exchange PoC is focused on validating telecoms operators as a unique source of scam-intelligence.

In that sense, the PoC is not simply another data-sharing platform. Rather, it represents an effort to establish telecoms operators as ecosystem risk-intelligence providers, capable of providing early-warning signals that help shift scam prevention from reactive response to proactive intervention. Learnings from the PoC strengthen the case for integrating telecoms intelligence more deeply into scam prevention frameworks, spanning financial services, digital platforms and the wider digital ecosystem.

3.2 Learnings from the pilot

The PoC pilot provides an opportunity to assess how a sustainable data-sharing ecosystem can be developed across five areas that directly address the challenges outlined above. These are:

1. governance frameworks that foster trust, purpose and accountability
2. alignment of leadership endorsement with middle-management execution
3. privacy-preserving mechanisms
4. data readiness and effectiveness, including data quality, timeliness, scale
5. commercial structures that incentivise early risk detection and measurable scam prevention outcomes.

Collectively, the learnings from these five areas provide a blueprint for evolving the PoC into a scalable, cross-sector, jointly governed data-sharing ecosystem capable of delivering proactive scam prevention at ecosystem scale.

3.2.1 Governance: collaboration should be built around trust, purpose and accountability

One of the most important learnings from the PoC is the need for a clear governance framework that aligns participants around a common purpose while providing safeguards for the responsible use of shared data. The pilot identified four mutual matches between the confirmed bad actors flagged by participants but also revealed a much larger pool of potentially unique suspicious identities. This suggests that the greatest value lies not in sharing already confirmed malicious actors, but in combining complementary intelligence to identify risks earlier and more effectively.

This has several implications for ecosystem governance:

- Participants require agreed definitions for scam categories, confidence levels and signal quality.
- Clear rules are needed to govern the permissible use of shared signals, data ownership and accountability for decisions informed by shared intelligence.
- Governance frameworks should support collaboration around suspicious indicators and emerging risks, rather than focusing exclusively on confirmed scam cases.
- Trust should be reinforced through transparency, auditability and clearly defined escalation and intervention processes.

A particularly important lesson is the need for a confidence-based framework that enables participants to share and act on suspicious indicators using graduated confidence scores, helping organisations assess risk and respond appropriately even when fraud has not yet been conclusively confirmed. Future exchanges should move beyond binary classifications of scams and instead incorporate graduated confidence scores that allow participants to respond in line with their own risk appetites and operational requirements. Lower-confidence signals should ordinarily support further verification or risk assessment rather than, by themselves, trigger adverse action. This approach would provide greater flexibility while maintaining consistent governance principles across the ecosystem.

The PoC also highlighted the importance of securing senior leadership support. Scaling up beyond a technical PoC requires stakeholders to understand the strategic value proposition, governance arrangements, liability considerations and pathway to measurable outcomes. Without strong executive sponsorship, organisations may struggle to justify participation, particularly when benefits are distributed across the ecosystem rather than accruing solely to the contributing organisation.

3.2.2 Organisation execution: aligning leadership endorsement with middle-management execution

A recurring lesson from the pilot is that senior executive commitment, while essential, is rarely enough to move data-sharing programmes forward. C-suite leaders often support multi-sector anti-scam initiatives in principle, recognising their strategic, reputational, regulatory and societal value. However, progress can stall when that intent moves into legal, compliance, data-governance and business-owner reviews, particularly where the return on investment is unclear or the initiative does not align with existing functional key performance indicators (KPIs).

Cross-sector data-sharing initiatives can therefore struggle to find an operational owner. Commercial teams may demand immediate revenue forecasts and clear monetisation timelines, treating collaborative threat intelligence like a conventional sales product rather than an enterprise risk-mitigation capability. Operational and risk teams may also hesitate to take responsibility: cybersecurity teams can see external scam disruption as outside their core mandate, while compliance and legal teams may view voluntary data exchange as a source of regulatory exposure, privacy liability and audit risk.

This execution gap reflects a deeper misalignment between strategic objectives and frontline incentives. Senior leaders focus on ecosystem-level risk reduction, trust and brand protection, while middle managers are measured against functional KPIs, liability control and compliance with statutory data-protection obligations. For legal or compliance teams, approving a new data-exchange model can appear to create asymmetric risk: the benefits are shared across the organisation and ecosystem, but any privacy breach or regulatory failure falls directly on their function. As a result, operational teams often default to caution and delays, treating voluntary signal sharing as a compliance risk rather than a business priority.

Overcoming this barrier requires translating executive sponsorship into clear cross-functional governance arrangements. Senior leaders should reduce the personal and departmental risk faced by middle management through clear legal guidance, aligned performance metrics and privacy-preserving architectures such as data sandboxes, while preserving each function's responsibility for appropriate legal, privacy, compliance and risk assessment. With clear institutional protection, strategic commitments to data sharing can move more quickly from executive intent to operational delivery.

3.2.3 Privacy: privacy-preserving collaboration is both necessary and feasible

The PoC demonstrates that meaningful scam-intelligence sharing can take place without exchanging raw personal data. Throughout the pilot, matching was conducted using privacy-preserving techniques, enabling organisations to collaborate while minimising privacy risks. However, the findings also indicate that scaling up the ecosystem will require more advanced privacy mechanisms to support increasingly sophisticated use cases.

A key learning relates to the need to validate whether suspicious numbers identified by operators are present on digital platforms. While this is critical to demonstrating ecosystem value, it requires comparison against potentially legitimate user accounts – datasets that are significantly more sensitive than lists of confirmed bad actors.

This has several implications for future privacy requirements:

- Privacy-enhancing technologies must support the analysis of larger and more sensitive datasets, potentially including legitimate user accounts where legally authorised, necessary and proportionate.
- Data clean rooms[9] and privacy-preserving statistical techniques may be needed to validate platform presence while protecting legitimate users.
- Privacy controls must evolve alongside ecosystem expansion to maintain participant trust, regulatory confidence and compliance with data-protection requirements.

9 Secure data-sharing environments that enable organisations, such as telecom operators, banks and digital platforms, to compare and analyse fraud signals without revealing sensitive customer information or transferring raw datasets between participants.

The recommendation to use key-based hashing for legitimate-user samples is particularly significant, as it demonstrates how privacy safeguards can be strengthened to support more advanced forms of collaboration. Enhanced privacy protections not only reduce regulatory and reputational risk, but also lower organisational barriers to participation and facilitate engagement with regulators and other stakeholders.

More broadly, the pilot highlights that privacy should not be viewed solely as a compliance requirement. Rather, it is a critical enabler of ecosystem-scale collaboration, allowing organisations to contribute richer and more valuable datasets while maintaining appropriate protections for customer information. As the ecosystem matures, robust privacy safeguards will be essential to unlocking broader participation and enabling more effective intelligence sharing across sectors.

3.2.4 Operational foundations: data quality, scale and timing are critical

The PoC reinforced that successful collaboration requires more than simply connecting datasets. Operational success depends on high-quality data, aligned methodologies and sufficient scale to generate meaningful and actionable insights. Several important operational learnings emerged:

- **Complementary signals create the greatest value:** The results suggest that telecoms operators and digital platforms observe different indicators of suspicious behaviour. Rather than replicating information that participants already possess, data sharing creates value by revealing blind spots and extending visibility across different stages of the scam lifecycle. This highlights the importance of combining complementary intelligence to create a more complete view of emerging threats.
- **Temporal analysis strengthens scam detection:** The findings also underscore the importance of chronological alignment between datasets. Understanding when a signal first appears can help identify where fraudulent activity originates and which participant has the earliest visibility of emerging threats. Future iterations should therefore place greater emphasis on time synchronisation and signal sequencing.
- **Scale, combined with data quality and robust validation, can increase confidence and analytical value:** While the pilot was intentionally limited in scope, the findings point to the need to expand data volumes, observation periods and participant numbers. Larger datasets will make it easier to distinguish genuine behavioural patterns from isolated anomalies and support more statistically robust conclusions, provided that data quality, representativeness, bias, error rates and freshness are appropriately assessed.
- **Legitimate user accounts may help measure value:** The pilot could not accurately measure the full extent of overlap between datasets because the analysis was largely limited to flagged records. Future iterations may consider incorporating representative samples of legitimate user accounts where a less intrusive alternative would not be adequate and where there is a clear legal basis, to measure overlap rates more accurately, assess ecosystem coverage and quantify the incremental value generated through collaboration.

3.2.5. Commercial foundations: the business value lies in prevention, not detection

Another important learning from the PoC is that the greatest value in data sharing does not come from exchanging information on actors that have already been confirmed as fraudulent, but from identifying suspicious actors before malicious activity is conclusively established and harm occurs. This insight has significant implications for how a sustainable data-sharing ecosystem should be commercialised.

Traditional data-sharing initiatives often focus on the exchange of known bad actors. However, the PoC suggests that such datasets offer limited incremental value, as participants are expected to act against confirmed threats independently. The greater opportunity lies in enabling earlier detection and intervention through the sharing of weak signals, risk indicators and emerging behavioural patterns that may point to fraudulent activity before it is fully realised.

The PoC highlights several key commercial requirements, including:

- a clear articulation of the value created for each participant
- defined frameworks for data ownership, responsibilities and liability management
- mechanisms to recognise and reward contributors of high-value intelligence
- commercial models that enable participants to create value from derived risk intelligence and preventative capabilities, rather than relying on the monetisation of underlying data
- a phased roadmap that links participation to measurable outcomes
- evidence that collaboration can reduce scam losses, improve consumer safety and strengthen digital trust.

The findings also highlight the need for clearer commercial relationships and value-realisation models if the initiative is to secure executive sponsorship and scale beyond the pilot stage. Participants must be able to understand not only how the ecosystem operates but also how value is created, distributed and sustained over time. Establishing this link between participation and outcomes will be critical to building a commercially viable ecosystem that encourages long-term collaboration and investment.

The PoC considered several categories of telecoms signals, including confirmed fraudulent numbers, suspicious prepaid SIMs, deactivated numbers that may still be linked to online accounts, user-reported scam numbers, suspicious traffic patterns and behavioural indicators associated with scams. The intention was not to create real-time access into operator systems, but rather to support periodic, secure and privacy-compliant sharing of relevant datasets.





04
Scaling up telecoms data sharing beyond pilots

The GSMA Data Exchange PoC demonstrates how value can be generated through privacy-preserving data sharing, allowing participants to contribute scam signals that reveal activity not visible to any single organisation. Importantly, the pilot showed that the greatest opportunity lies in combining diverse observations to identify suspicious activity earlier in the scam lifecycle, enabling more proactive and effective intervention. However, scaling up beyond pilot environments will require stronger governance frameworks, enhanced privacy protections, common protocols and sustainable commercial incentives that support long-term participation.

Looking ahead, the next phase of ecosystem development should focus on transforming collaborative data sharing from a series of controlled pilots into a trusted intelligence infrastructure. Achieving this will require broader participation from telecoms operators, digital platforms, financial institutions and other ecosystem stakeholders, supported by privacy-enhancing technologies, automated intelligence-sharing mechanisms and, ultimately, API-enabled collaboration.

By building on the lessons from the PoC, the industry has an opportunity to create a sustainable ecosystem that strengthens digital trust, enables earlier scam detection and supports coordinated intervention across the wider digital economy. The following recommendations outline the key actions that digital ecosystem participants can take to unlock this potential.

4.1 Align stakeholders around shared incentives and a clear commercial vision

One of the most important lessons from the PoC is that technical feasibility alone is insufficient to create a sustainable data-sharing ecosystem. The greater challenge lies in aligning diverse stakeholders around a shared value proposition. Telecoms operators and other ecosystem participants all incur costs, risks and operational commitments when contributing data, yet the benefits are often distributed unevenly across the ecosystem. Without aligned incentives, participation is likely to remain fragmented and difficult to scale up.

The PoC therefore highlights the importance of developing a commercial model that rewards collaboration, recognises participant contributions and links engagement to measurable scam-prevention outcomes. Establishing a clear value proposition for all stakeholders will be critical to securing long-term participation and investment.

Given this context, the next phase of ecosystem development should align stakeholders around a shared commercial vision focused on scam-prevention outcomes, rather than data exchange as an end in itself. This will require transparent value attribution mechanisms, the recognition of high-quality signal contributions and a commercial roadmap that evolves from collaborative learning and value validation to shared intelligence services and outcome-based value creation (see Table 3).

Table 3: Examples of outcome-based value creation

Outcome	Example of value metric
Scam prevented	Monetary losses avoided
Earlier detection	Reduction in response time
Signal contribution	Verified intelligence leading to interventions
Ecosystem participation	Improved coverage and detection rates
Consumer protection	Reduced victimisation rates

Source: GSMA Intelligence

This approach shifts the conversation from who owns the data to how much harm can collectively be prevented, recognising that different stakeholders derive value in different ways. Telecoms operators benefit from reduced scam traffic and regulatory pressure; digital platforms gain from improved trust and safety and lower moderation costs; financial institutions benefit through reduced scam losses and compliance costs; and regulators and governments benefit from improved consumer protection and better visibility of emerging threats.

Recognising these differing incentives is critical to building a sustainable ecosystem. While participants may realise value in different ways, they all share a common interest in reducing scams, strengthening digital trust and improving the safety of the digital economy. Commercial models should therefore balance individual benefits with collective outcomes, taking account of the practical challenges of attributing and measuring scam-prevention results.

Meanwhile, the PoC also demonstrated that organisations are more willing to collaborate when they have confidence that shared data will be used only for agreed purposes and protected by appropriate safeguards. As participation expands beyond telecoms operators to include digital platforms, financial institutions and other ecosystem stakeholders, stronger governance frameworks and technical controls will be required to ensure responsible data use, maintain participant confidence and support long-term collaboration.

The data exchange agreements and governance structures developed through the PoC provide a strong foundation for this next phase of ecosystem development. However, scaling up the model will require clear rules on data access, permissible use, accountability and oversight, supported by transparent processes that allow participants to verify how shared intelligence is used. Establishing these trust mechanisms will be critical to encouraging broader participation and enabling the exchange of increasingly valuable intelligence across sectors.

4.2 Drive a shift in organisational mindsets to support collaborative data sharing

Some organisations continue to view data as a proprietary asset that should be protected. However, the PoC showed that telecoms operators, digital platforms and other stakeholders often hold unique but complementary perspectives on scam activity. The greatest value emerged when these different signals were combined, revealing risks and patterns that would not have been visible to any single participant. Unlocking this potential requires a shift from isolated risk management towards collective ecosystem defence.

For a telecoms data-sharing ecosystem to succeed, organisations need to consider data stewardship alongside data ownership, with an ecosystem-wide goal: using shared intelligence to reduce harm, protect consumers and strengthen digital trust while respecting applicable legal duties, customer expectations and legitimate commercial interests. Achieving this shift will require strong leadership commitment and cross-functional alignment. The PoC shows that a mindset change is unlikely if collaborative data sharing is treated only as an operational issue for scam, compliance, legal or security teams. Executive sponsorship is needed to position participation as a strategic priority, align objectives across functions and overcome organisational inertia.

Leaders also need to redefine success beyond operational metrics, such as the volume of data exchanged or the number of alerts generated. The real measure of success is the impact created through collaboration: scams prevented, harm reduced, consumers protected and trust strengthened. Aligning incentives and performance measures around these outcomes can help embed collaboration into organisational priorities. To build confidence, leaders should communicate pilot successes, show how privacy and governance safeguards manage risk and reinforce that effective scam prevention increasingly depends on coordinated action across sectors.

A key strategic implication of the pilot is that the greatest value emerges when multiple participants contribute complementary intelligence. While bilateral exchanges can generate useful insights, they capture only part of the visibility needed to understand and disrupt scam across the ecosystem. Multi-directional data sharing allows signals to flow among telecoms operators, digital platforms, financial institutions, payment providers, regulators and other trusted participants, creating a network effect in which the value of collaboration increases as participation grows. This requires organisations to move beyond siloed approaches to scam prevention and adopt a model of collective defence, where shared intelligence is used to build a more complete picture of scam activity and support earlier, more coordinated intervention.

4.3 Creating the enabling environment for data sharing

Governments should play a central role in enabling, convening and coordinating trusted data sharing across the ecosystem, rather than acting as central repositories or brokers of industry data. Their role is to bring together the industry, technology platforms, financial institutions and other relevant stakeholders to establish common objectives, governance frameworks and practical mechanisms for collaboration. In many cases, the most effective arrangements allow information to flow directly between authorised participants, supported by clear rules, legal certainty, technical standards and appropriate oversight. Governments can provide the policy and regulatory foundations that give participants confidence to share data responsibly. They can do this alongside actively facilitating industry-led solutions and avoiding models that unnecessarily concentrate sensitive data in one location or create operational dependencies.

Legal and regulatory uncertainty remains one of the biggest barriers to scaling up data-sharing initiatives. Organisations may be willing to share data that protects consumers and strengthens trust but remain unclear about how privacy, competition, telecoms and other legal obligations apply in practice. Governments can address this through clear guidance, safe harbours and exemption frameworks that give organisations confidence to participate in approved data-sharing arrangements in good faith.

Policymakers should also consider targeted exemption frameworks or regulatory sandboxes that allow trusted participants to test new data-sharing models in controlled settings. These mechanisms can help identify legal, operational and technical barriers before wider deployment while maintaining appropriate safeguards. The lessons generated can then inform more permanent policy and regulatory approaches.

Scaling up data sharing will also require sustained cooperation between governments, telecoms operators, digital platforms, financial institutions and other ecosystem participants. No single organisation has a complete view of digital threats and no sector can address them alone. Governments are therefore well placed to convene and facilitate voluntary collaboration, align incentives, promote common data formats and support trusted frameworks for responsible data sharing.

Ultimately, moving from pilots to operational scale depends on an environment that gives organisations the confidence, legal certainty and governance mechanisms to collaborate. Governments have a central role in enabling this transition, not by owning the data, but by creating the conditions for trusted and responsible data sharing to flourish.

Call to action

Unlocking the next phase of collaborative scam prevention

Scams have become an ecosystem-wide challenge that no single organisation can tackle alone. Telecoms data can provide valuable early-warning intelligence, particularly when combined with complementary signals from across the digital ecosystem.

This creates an opportunity to develop trusted intelligence infrastructure that identifies risks earlier, enables coordinated intervention and strengthens digital trust across Asia Pacific. The GSMA Data Exchange PoC shows that privacy-preserving collaboration is both feasible and valuable. It also demonstrates that sustainable data sharing depends on commercially rational participation: incentives can make contributing trusted intelligence more valuable than operating in isolation.

The next phase is no longer about proving that data sharing works; it is about scaling it up. This will require organisations to move from data ownership to data stewardship, recognising that collective intelligence creates greater value than isolated information. It will also require broader participation from telecoms operators, digital platforms, financial institutions, policymakers and regulators, supported by common standards, trusted governance, privacy-preserving technologies, AI-enabled analytics and API-based intelligence sharing.

The call to action is clear:

- **Governments and regulators** should provide the policy, legal and regulatory foundations for responsible data sharing while actively promoting and convening collaboration across the industry and wider ecosystem around common objectives and protocols. They should support trusted initiatives through safe harbours, targeted exemptions and clear accountability frameworks while encouraging industry-led data sharing, rather than acting as central repositories or brokers of industry data.
- **Telecoms operators, digital platforms and financial institutions** should deepen participation in trusted cross-sector data-sharing initiatives, subject to applicable law, business judgement, technical feasibility, proportionate costs, reciprocal contributions, clear liability allocation, confidentiality protections and effective redress mechanisms. They can appropriate threat signals, adopting common data formats and taxonomies, implementing privacy-preserving practices and supporting shared governance frameworks that enable essential intelligence to be exchanged safely, securely and at scale.
- **Cross-border and multinational organisations** should take a proactive role in enabling trusted cross-border and cross-sector data sharing where this can support scam prevention outcomes. This may include convening ecosystem participants, facilitating the responsible exchange of threat signals, promoting common governance approaches and extending collaboration beyond telecoms, financial services and digital platforms to other relevant stakeholders. Such initiatives can help address coordination gaps while government frameworks continue to evolve, complementing rather than replacing the role of public authorities.
- **Industry bodies** should work with their members, private-sector players and government partners to develop a trusted, industry-led data exchange ecosystem. For example, the GSMA Data Exchange PoC demonstrates how the GSMA convenes stakeholders, strengthens regional coordination, promotes interoperability and shares best practices to accelerate adoption across Asia Pacific.

GSMA
Intelligence

gsmaintelligence.com