



PERSPECTIVE

The Permission Nobody Used

Twenty-five years of safe harbour, and the risks it left in place.

Leslie Falvey · September 2026

Everyone who has ever asked why banks do not share what they know about fraud has been given the same answer. The lawyers will not allow it. Share a suspicion about a customer and you invite a claim for breach of confidence, so the file stays shut. It follows that the fix is a safe harbour: a law saying you may share, and you cannot be sued for it.

Two governments have now done exactly that. The United States in 2001, the United Kingdom in 2024. In both cases the sharing did not follow. Not because firms are obstinate, but because both statutes removed the risk that was easy to remove, left one in place deliberately, and never addressed a third at all.

What is currently believed

The orthodoxy is reasonable and widely held. Fraud defence is weakened because each institution sees only its own slice. One bank sees the outbound payment, another sees the account receiving it, a telco sees the call that set it up, a platform

sees the advertisement. Nobody sees the whole. Pooling the slices would let all of them act sooner. Armidale's 2026 consumer survey for the GSMA bears this out: 49% of scam victims were reached on more than one channel, and victims who reported took their case to nearly two organisations on average, 36% to a financial institution, 36% to the police, 32% to a digital platform and 19% to their telco.

What stops it, on this account, is legal exposure. A firm that shares a suspicion has broken a duty of confidence to its customer and can be sued. The customer may be innocent. The suspicion may be wrong. No compliance function will accept that risk without protection, and no amount of goodwill overcomes it.

So the ask, in every consultation of the past two decades, is a safe harbour. Remove the liability and the information will move, because the reason it does not move is that firms are afraid.

This is the right diagnosis of one obstacle and the wrong diagnosis of the decision.

The evidence

The United States removed the risk in 2001 and a fifth of the registrants used it

Section 314(b) of the USA PATRIOT Act lets financial institutions share information with each other about suspected money laundering and terrorist financing, with a safe harbour from liability. Registration is voluntary and free. By the end of 2020, more than 7,000 institutions had registered.

The Financial Crimes Enforcement Network's own figures on what they then did with it:

- 1,523 institutions, about 22% of registrants, referenced the provision in any suspicious activity report that year
- 17,384 reports referenced it, a fraction of a percent of annual filing volume
- Six registrants were associations of financial institutions, meaning the collective structure the statute expressly permits was used six times nationally

Twenty-five years after the liability was removed, four out of five institutions that signed up for the protection had not used it.

The United Kingdom removed the same risk and kept the one that matters

The Economic Crime and Corporate Transparency Act 2023 created an equivalent power in January 2024. Sections 188 and 189 disapply the duty of confidence and civil liability to the customer for firms sharing to prevent economic crime.

Then both sections say this:

“Nothing in this section requires or authorises a disclosure of information that would contravene, or prevents any civil liability arising under, the data protection legislation.”

Breach of confidence, removed. Tort, removed. Data protection, untouched, deliberately, on the face of the Act.

All four are drawn around the wrong industry

Those two are not the only attempts. Since 2024 the European Union and Singapore have created their own channels for firms to share financial crime information with each other.

Instrument	Who may share	About what
United States, PATRIOT Act s.314(b), 2001	Financial institutions under the Bank Secrecy Act	Money laundering and terrorist financing. Extension to fraud clarified only in June 2026
United Kingdom, ECCTA ss.188-189, January 2024	AML-regulated firms	Economic crime, with data protection liability expressly preserved
Singapore, COSMIC, 2024	The central bank and the six largest banks	Misuse of legal persons, misuse of trade finance, proliferation financing
European Union, AMLR Article 75, from July 2027	Obligated entities	Money laundering and terrorist financing obligations, and only for customers already identified as higher risk

Table 1. Statutory channels for competitors to share financial crime information. Compiled from each instrument as cited in the sources note.

Every one is confined to regulated financial institutions. Not one reaches a telecommunications operator, a messaging service, a social media platform, a domain registrar or an advertising network. Singapore's police report that online platforms were used to reach the victim in 84.1% of scam cases.

And every one is scoped to money laundering rather than fraud. Singapore's COSMIC is the clearest case, because it is not a permission but a working system: a centralised platform built by the central bank with the six largest banks, whose three stated focus areas are the misuse of legal persons, the misuse of trade finance, and proliferation financing. Consumer fraud is not among them.

The world has now built at least four channels for competitors to share information about financial crime. Consumer fraud is outside the scope of all of them.

And nobody has said whether competitors may discuss it at all

Both statutes deal with confidentiality, and the British one deliberately declines to deal with data protection. Neither addresses the question that comes up first in any cross-industry fraud meeting, which is whether the people in the room, who compete with each other, are allowed to be there.

No competition authority appears to have answered it. No guidance, exemption or comfort of any kind could be located, in any jurisdiction, on how competing firms may share fraud intelligence without breaching competition law. The British government guidance accompanying the 2023 Act runs to considerable length on data protection and legal privilege, and does not mention competition law once.

The contrast is the finding. The Competition and Markets Authority has published dedicated guidance telling competitors how they may collaborate on environmental sustainability without falling foul of the same rules. It built a bespoke instrument, for one policy priority, because uncertainty was chilling collaboration that the government wanted to happen.

Fraud accounted for 4.2 million of the 9.4 million crimes estimated by the Crime Survey for England and Wales in the year to March 2025, close to half of everything it measures, and the highest figure since it began counting fraud in 2017. It has no equivalent.

Why it happens

A safe harbour removes the risk its drafter can see. It does not remove the risk the person making the decision is actually weighing.

Consider what a compliance officer is choosing between. Breach of confidence is a claim brought by one customer, about one disclosure, quantifiable, insurable, and defensible on the facts. It is a bad afternoon. Data protection is different in kind. It is a continuing obligation, enforced by a regulator rather than a claimant, assessed across a whole practice rather than a single act, and capable of producing a fine calculated against global turnover. One is a lawsuit. The other is a supervisory relationship.

Removing the first while expressly preserving the second does not change the answer, because the second was the reason. The statute reads as permission. Inside the firm it reads as a permission that still requires a lawful basis, a documented necessity assessment, an impact assessment, and a defence of the decision to a regulator later. The work does not reduce. Only the litigation risk does, and the litigation risk is simply not the binding constraint.

The caution is not coming from customers. In the same survey, 79% of consumers were comfortable with their financial institution holding and using their data to detect fraud, and 69% with their telco. Digital platforms, which carry the largest share of the approach, held the least permission, at 60%.

And on the third risk there is nothing to weigh at all, because no regulator has said anything. Silence is not permission. A general counsel reading silence advises caution, which is the correct advice but the wrong outcome.

There is a further reason, and it survives even if every legal question is solved. Shared intelligence has the economics of a public good. A firm that contributes bears the cost of extracting, cleaning and sending the data, and accepts the risk of being wrong. The benefit accrues to everyone in the pool, including firms that contribute nothing. The rational position for any individual participant is to join,

receive, and send as little as possible. That is exactly the pattern the American numbers describe: seven thousand registrations, fifteen hundred users.

Voluntary schemes cannot fix this, because voluntariness is the mechanism producing it.

The strongest objection

Twenty-two per cent is not zero, and adoption of anything takes decades. The counterfactual matters too. Nobody knows what sharing would have looked like without the safe harbour, and it may be that 1,523 institutions sharing is a substantial improvement on a baseline of almost none. The American regulator also clarified in June 2026 that the protection extends to suspected fraud even where money laundering has not been identified, which removes a real ambiguity. Uptake may now rise. Judging a statute at twenty-five years and calling it a failure may simply be judging it before the clarification that made it usable.

That is fair, and the regulator's own participation data will settle it within two years. If the share of registrants using section 314(b) rises materially now that fraud is expressly covered, the binding constraint was scope rather than data protection.

What follows

FOR GOVERNMENTS AND REGULATORS

If you legislate a safe harbour, it must reach the risks that decide the question. A provision that removes confidentiality liability and expressly preserves data protection liability has not made sharing lawful. It has made it slightly less litigious. Either create a lawful basis for fraud-prevention sharing on the face of the statute, or state openly that you have chosen not to, and explain why.

Then do the thing that costs nothing. Ask your competition authority to publish guidance on fraud-prevention collaboration, on the model it has already used for environmental agreements. This requires no legislation, no new body and no budget. It requires a regulator to write down what it already thinks. That it has not

been done anywhere is the clearest available evidence that fraud is treated as an industry problem rather than a public one.

And extend the eligible parties beyond the payment industry to the channels where the approach is made. Intelligence drawn only from the paying end of the chain is missing the half that would have prevented it.

FOR INDUSTRY

Stop asking for comfort and start expecting a duty. Every scheme examined here that produced a measurable outcome had a compulsory element. The voluntary ones produced activity reports, not outcomes.

Sources and method

USA PATRIOT Act section 314(b), and the Financial Crimes Enforcement Network's Section 314(b) Fact Sheet of June 2026, superseding the December 2020 version. FinCEN, Information Sharing Insights: 314(b) Participation and Reporting, covering calendar 2020. Economic Crime and Corporate Transparency Act 2023, sections 188 and 189, in force 15 January 2024, quoted from the statute, together with the accompanying joint government guidance. Monetary Authority of Singapore, on COSMIC. Regulation (EU) 2024/1624, Article 75. Competition and Markets Authority, Green Agreements Guidance. Singapore Police Force, Annual Scam and Cybercrime Brief 2025, for the platform contact share. Office for National Statistics, Crime in England and Wales, year ending March 2025, for the fraud and total crime figures. Armidale for the GSMA, ASEAN Consumer Scam Report 2026, for the channel, reporting and data-permission figures.

A fifth jurisdiction, Australia, is sometimes listed as having enacted comparable peer-to-peer information-sharing legislation. No such provision could be located, and the Australian reforms of this period concern the scope of anti-money-laundering obligations rather than information sharing between firms.

No figure in this report has been rescaled, modelled or extrapolated. One is arithmetic from figures in the cited source and is shown in the text: 1,523 of more than 7,000 registrants.

About the author

Leslie Falvey is the founder of Armidale, a Singapore advisory firm, and author of the GSMA ASEAN Consumer Scam Report 2026, now in its third edition across six ASEAN markets and India. His work follows how consumers encounter, report and resolve scams, and treats fraud as an economic harm whose largest costs fall outside both the victim and the firm that failed to resolve the case.

About Armidale

Armidale is a Singapore advisory firm working at the intersection of payments, fraud and digital commerce, combining primary consumer research with strategy and execution for operators, financial institutions and industry bodies.

© 2026 Armidale Pte. Ltd. · Published September 2026 · armidale.co · Provided for information and does not constitute legal, financial or security advice.