FDX Global Summit 2026 | Open Finance Risk Report

Who Holds the Risk in Open Finance

— and What Is That Risk Anyway?

Open finance is accelerating. The risk model hasn't kept pace. Data moves through more systems, more businesses, and more business models than ever before. This panel report captures the unvarnished debate from four leading voices across the open finance ecosystem — a banker, a lawyer, an aggregator & third-party provider, and an infrastructure provider — on what the risk actually is, where liability should sit, and what it will take to build an ecosystem that doesn't break.

Invela™

The Perspectives

Chaired by Alex Johnson, CEO, Fintech Takes

Aakash Tuli

Sr. Director of Architecture & Emerging Technology, Zions Bank

The bank perspective: data security, reputational risk, and the operational burden of consumer-permission data.

Geoff Scott

Chief Risk and Compliance Officer, Aerosync & Aeropay

The aggregator and third-party provider perspective: competitive risk, consumer friction, and the limits of vetting at scale.

George Anderson

CEO, Ninth Wave

The infrastructure perspective: technical complexity, chain-of-custody, and the case for governance in the infrastructure layer.

Todd Taylor

Co-Head IP & Commercial Technology, Moore and Van Allen

The regulatory and legal perspective: TPRM obligations, Reg E, GLBA, and the role of industry standards where regulation falls short.

1

PART ONE

Defining the risk

Before debating who holds the risk, the panel spent significant time on a more fundamental question: what exactly is the risk? The answer, it turns out, is not a single thing. It is a stack of distinct, compounding risks — each visible from a different position in the ecosystem.

1. Data Security and Privacy Risk

Aakash Tuli opened with the risks that banks see most directly. Screen scraping — while declining — remains live. When customers share credentials with third parties, those credentials are stored by entities that carry none of the regulatory obligations banks do. A breach at a fourth party doesn't just mean data loss; it can mean full account access and actual monetary loss.

"There's no data prevention requirement on third parties and fourth parties — they might store data, and the risk stays on for a very long time. Unlike if the banks were storing the data."

— Aakash Tuli, Zions Bank

Even with APIs — which are materially more secure than screen scraping — standardization gaps and residual vulnerabilities remain. The panel noted that customers who stop using an app often assume their data has been deleted. Frequently, it has not. There is no regulatory mechanism compelling third parties to purge data when a consumer relationship ends.

2. Third-Party Risk Management (TPRM) at Scale

Todd Taylor traced the regulatory obligation. The 2023 interagency TPRM guidance from the Office of the Comptroller of the Currency (OCC), Federal Deposit Insurance Corporation (FDIC) and Federal Reserve requires banks to put processes in place to manage risk across any "business arrangement" with a third party — a term broad enough to cover every fintech that a bank's customers choose to connect with, regardless of whether the bank had any role in selecting that fintech.

"The notion that third-party risk management can be applied, if you're a bank, to vendors that you had no role in choosing or vetting — that's what we're talking about with a framework really created to envision vendor relationships."

— Alex Johnson, Fintech Takes

The practical consequence: banks are theoretically responsible for managing the risk posed by thousands of fintechs they did not select, cannot fully vet, and have limited leverage over. The 2023 guidance superseded OCC FAQs from 2020 that had explicitly flagged data-aggregator relationships as a risk requiring protocols — but the underlying expectation persists.

3. Competitive and Consumer Friction Risk

Geoff Scott reframed the conversation. The operational and compliance risks are real, but so is the risk of over-correcting. Consumers expect data portability to work. A financial institution that makes it too difficult — or places so much friction into the process that connectivity breaks — pays a competitive price.

"If you're a large or medium credit union and you're not enabling your customers to get the access they want, you're going to be in trouble."

— Geoff Scott, Aerosync & Aeropay

Scott also flagged the structural impossibility of the current model: a full InfoSec review of a potential partner involves 200 questions and five people over multiple weeks. That is not achievable in real time, as a customer attempts to link an account. The vetting burden is real — but so is the cost of imposing it at the point of consumer interaction.

4. Technical Complexity and Chain-of-Custody Risk

George Anderson offered the infrastructure view. Open finance is a chain, and risk travels with the data along that chain. A consumer using a budgeting app may not know their data is passing through an aggregator, then another aggregator, then bank infrastructure, before reaching the bank's system of record. At each hop, questions multiply.

THE CHAIN-OF-CUSTODY PROBLEM	
Consent provability	Can each party in the chain prove the consumer actually authorized this specific use case?
Data integrity	How does anyone know the data was not modified in transit?
Standardization	Without normalized data formats, downstream applications receive inconsistent inputs.
Operational accountability	When something breaks, every party points to another. The consumer calls the bank; the bank says call the aggregator; the aggregator says call the fintech.

Anderson made the problem vivid: when his wife encountered a Venmo payment failure, she called the bank. The bank told her to call the aggregator. There was no clear point of accountability.

5. Reputational and Operational Risk for Banks

Tuli returned to the bank's position. When a consumer links a third-party app to their bank account, they assume the bank has vetted and endorsed that app. That assumption is generally wrong. But the bank still owns the relationship in the consumer's mind. When things go wrong, call volumes go up, resolution times lengthen, and the bank's reputation absorbs the damage — regardless of where the fault actually sits.

6. Regulatory Liability Overlap: Reg E, GLBA and the Gaps Between Them

Todd Taylor closed the risk taxonomy section with a regulatory mapping. Where screen-scraped or compromised credentials lead to unauthorized electronic fund transfers, banks face potential Reg E liability — even when the breach occurred at a third-party fintech or aggregator. The final 1033 rules did not resolve this; they pointed back to existing frameworks.

The Gramm-Leach-Bliley Act (GLBA) obligation adds a further layer: banks must maintain a reasonable written information security program covering data under their control. Once data leaves the bank, the GLBA argument becomes contested. But regulators have not formally released banks from the expectation that they scrutinize what happens to customer data after they share it.

> "The challenge is, when we looked at the last set of 1033 rules that came out, that question was sort of left to the existing rule framework. Banks were told, in some cases, you may even have to make payment initiation information available to third parties — and yet you are going to have to fall back on old regulations to determine the allocation of liability if there was a compromise."
>
> **— Todd Taylor, Moore and Van Allen**

2

PART TWO

Where Liability Should Sit — and How to Get There

With the risks mapped, the panel turned to the harder question: given where risk actually sits, where should liability sit? And what does a workable accountability framework actually look like in practice?

The "Veil of Ignorance" Principles Test

Alex Johnson asked each panellist to design a principles-based liability framework from scratch — setting aside existing frameworks, regulatory politics, and commercial interests. Four distinct but complementary answers emerged.

FOUR VIEWS ON WHERE LIABILITY SHOULD SIT	
George Anderson Ninth Wave	Governance needs to move into the infrastructure layer. Use cases should be tightly defined — like a time-limited credit file pull. All parties should agree on a 'technical contract' governing the data exchange, with positive enforcement built into the infrastructure itself.
Aakash Tuli Zions Bank	End-to-end contractual liability, with shared responsibility at each hop. Banks provide secure access; fintechs and aggregators take responsibility for managing data securely on their side. Convert the many-to-many problem into a one-to-one problem through an intermediary abstraction layer.
Geoff Scott Aerosync & Aeropay	Ultimately, it is the consumer who suffers when data is lost or misused — and consumers are often not well-equipped to track all the parties holding their data. Liability frameworks must reflect that reality, not assume sophisticated consumer judgment.
Todd Taylor Moore and Van Allen	The bank's liability should be bounded: validate the requesting party, provide a secure data pathway, confirm secure delivery — and then liability should transition to the receiving fintech or aggregator. Clear handoff, clear accountability. Today's contractual approach provides the framework in theory; the practice is inconsistent.

"Once it's over the other side of the fence, the fintechs, the aggregators, the consumer — they should allocate that liability. That's the theory. And I think it's a pretty fair theory."

— Todd Taylor, Moore and Van Allen

The Scalability Problem: Why One-by-One Vetting Has Already Failed

A consistent theme across all four panelists: the current model — in which each bank individually vets every third party its customers choose to connect with — has already broken down. It was not designed for an ecosystem of thousands of fintechs, with AI-enabled entrants arriving daily.

"There is a need for, almost like an aggregator — an abstraction layer that allows risk management to take place and set the boundaries. Even if we could do risk analysis against all the fintechs, we don't necessarily have the leverage to make smaller providers adopt higher security standards."

— Aakash Tuli, Zions Bank

Scott echoed the point from the aggregator side: without a centralized backstop or audit function, aggregators are effectively self-policing their third-party relationships based on company culture and judgment, not external requirement. That is not a durable risk management model.

The Limits of Contractual Risk Management

George Anderson delivered the most direct assessment of contractual approaches:

"If you ever pull a contract out of a drawer after you sign it, it's probably a bad day. Contracts are necessary — but the contract is not going to help you when there's a suspected breach and you tell the counterparty they owe you $300 million and they say: great, we don't have it."

— George Anderson, Ninth Wave

Contracts establish the rules of the road. They do not provide real-time risk intelligence, prevent breaches from occurring, or guarantee financial recovery when liability is triggered. Anderson pointed to the analogy of dynamic credit rating: what the ecosystem needs is something closer to a Rapid Ratings-style assessment — continuous, standardized, and actionable — rather than point-in-time due diligence locked in a vendor questionnaire.

Industry Standards as the Only Viable Bridge

With regulation either absent or unable to move at ecosystem speed, all four panelists converged on the same conclusion: industry standards and private network rules are not a fallback. They are the primary mechanism for allocating risk in open finance — and the sector needs to treat them that way. Todd Taylor drew the historical parallel most sharply. Payment networks — card schemes, ACH — long ago built liability allocation rules that govern who bears the cost when something goes wrong. PCI DSS created a shared security baseline. The open finance ecosystem needs its equivalent.

"Even the rules and frameworks that banks operate under from a risk management standpoint tend not to be detailed or prescriptive. Instead, there's a recognition that there has to be a gap-filler — whether those are ISO rules, data security frameworks, or payment network allocation rules. The obligation is on all of us to figure that out if regulators aren't going to."

— Todd Taylor, Moore and Van Allen

The panel noted that Director Chopra himself — in conversations after the 1033 rule — indicated the Consumer Financial Protection Bureau (CFPB) did not view it as its role to define where liability sits across every scenario. That responsibility has effectively been delegated, by default, to the industry.

3

PART THREE

What's at Stake if We Get This Right

Alex Johnson closed the session with a deliberate pivot toward optimism: if the industry solves the risk and liability problem, what does the upside actually look like?

Todd Taylor: The market will continue to grow regardless of whether we solve the governance problem. Demand for open finance use cases is not abating. The optimistic read is that demand creates commercial pressure to find solutions. The less optimistic read is that the 'solution' will emerge messily, after things go wrong.

Geoff Scott: Market momentum is real, and many participants genuinely care about protecting consumer data and maintaining strong standards. The desire to be trusted partners to banks is itself a structural incentive. But the plumbing still leaks, and there are too many players with insufficient control.

Aakash Tuli: Empowered consumers. A partner ecosystem with genuine confidence in security. Banks that can say yes to open finance without carrying unmanaged risk. The community-based approach — where risk management scales through shared infrastructure — is what unlocks this.

George Anderson: The current conversation focuses almost entirely on retail banking. The real prize is business banking — where the bulk of assets sit and where open finance has barely begun. Get the governance model right for retail, and you have the foundation for a much larger transformation.

> "If the infrastructure just worked 10% better than it does today, the number of use cases that unlock is enormous. Infrastructure has such a high bar — and we can solve that last gap."
>
> **— Alex Johnson, Fintech Takes**

Five Things the Industry Must Now Confront

Five structural challenges stand out as requiring deliberate industry action — not further deferral.

THE FIVE STRUCTURAL CHALLENGES	
1. Vetting at scale	No individual bank, aggregator, or regulator can vet thousands of fintechs in real time. The model requires a shared, centralized risk assessment layer — analogous to credit rating, but purpose-built for open finance participants.
2. Liability handoff clarity	The ecosystem needs explicit, enforceable principles for when liability transfers between parties as data moves through the chain. Today this is handled by contract, inconsistently, and often untested until something goes wrong.
3. Technical contracts	Governance needs to be embedded in the infrastructure itself: defined use cases, time-limited consents, chain-of-custody verification, and automated enforcement — not just legal agreements that sit in a drawer.
4. Consumer data lifecycle	No regulatory mechanism currently compels third parties to delete consumer data when a relationship ends. This is an unresolved risk that grows with every new app connection.
5. Standards before regulation	Waiting for prescriptive regulatory rules is not a strategy. The industry must build its own PCI DSS equivalent for open finance — with shared security baselines, liability allocation rules, and participant assessment frameworks.

Invela™

About Invela

Invela is building the risk management network infrastructure for open finance — across the US, UK, and Canada. Our platform addresses the structural challenges this panel identified directly: standardized accreditation, dynamic real-time risk monitoring, and an insurance-backed warranty that provides the financial backstop for ecosystem participants.

Invela serves banks, credit unions, aggregators, and third-party fintechs that need to move from one-by-one vetting to scalable, standardized, continuously-monitored risk management.

We are the confidence layer the ecosystem has been asking for.

invela.com

This report was produced from the FDX Global Summit panel "Who Holds the Risk in Open Finance — and What Is That Risk Anyway?"