UNITED KINGDOM | WHITE PAPER

From fragmentation to federation: Invela is building scalable defences for the UK's Smart Data ecosystem

Invela™

Open Finance Covered

Table of Contents

Executive summary

The UK's smart data ecosystem is at a pivotal moment. With the passage of the Data Use and Access Act in Summer 2025, government has laid the legislative foundations for a data-driven economy – building from open banking to open finance and beyond - based on consumer empowerment, market innovation, and public benefit. Yet while the open banking ecosystem is expanding rapidly, its defences are not yet fully developed. If the ecosystem continues to scale to open finance and open data without robust, coordinated defences in place, risks will proliferate, cyber criminals will exploit gaps, and the fragile currency of public trust will erode - threatening not just consumer confidence, but the legitimacy and potential of the smart data economy.

This paper sets out how to build strong defences which manage risks, exclude bad actors, and federate resilience.

Executive Summary Continues

Today, banks and building societies are the cornerstones of the open finance ecosystem but are concerned about the potential for fraud or data breaches arising from third-party provider data access – particularly when factoring in those fourth, fifth and nth party providers that connect into the ecosystem via third-party providers. They are starting to recognise this as a risk register item, because they worry that they carry the lions' share of the liability for fraud and data breach and misuse, unsure as to whether, for example, a third-party provider's Professional Indemnity Insurance would translate into compensation to cover the bank or building society's cost of remediation. And that's before considering brand impact.

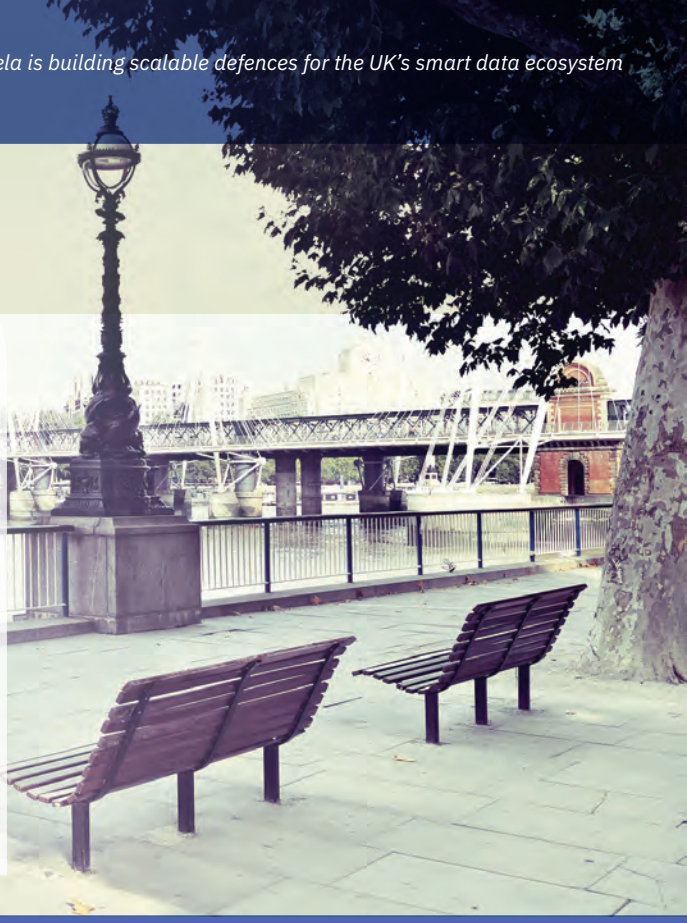
Aggregators, operating as intermediaries, know they face operational risk and reputational exposure. Third-party providers understand that they run the risk of being compromised by malicious actors without always having the depth of experience or pocket to adequately defend themselves. Consumers risk exposure to fraud or the consequences of a data breach. Meanwhile, regulators and legislators recognise that they own the blueprint yet rely on industry to deliver the government's ambition.

Core to building a fully effective and resilient ecosystem is Invela's solution, Open Finance Risk Management, which builds three lines of defence:

- **Rigorous open finance-specific accreditation** of aggregators and third-parties.
- **Dynamic, real-time risk monitoring** to alert banks, building societies and aggregators to issues as they occur, empowering them to revoke a third-party provider's data access until data breach and misuse or fraud issues are resolved.
- **Aligned incentives** which transfer economic responsibility for risk to those third-parties which introduce it to the ecosystem, via insurance-backed warranty.

Invela's value resonates across the ecosystem. Banks and building societies gain systemic visibility, actionable early warnings, and risk transfer – and a reduction in exposure to cybercrime and the associated brand impact. Aggregators increase downstream control and operational resilience. Third-party providers increase operational resilience and network legitimacy. Consumers benefit from frictionless protection and empowered participation. And legislators and regulators benefit from industry stepping up to work alongside them as implementation partners.

The smart data ecosystem can only scale safely if risks are addressed, bad actors excluded and trust earned. And industry is stepping up to the plate; Invela is delivering a simple, elegant solution – Open Finance Risk Management - to help the smart data ecosystem scale and thus to realise the ambitions of the Data Use and Access Act.



Legislative backdrop

In the United Kingdom, third-party providers directly accessing consumers ' bank accounts - Account Information Service Providers (AISPs) and Payment Initiation Service Providers (PISPs) - are supervised by the Financial Conduct Authority. Account access is always subject to consent of the account holder, and both AISPs and PISPs are required to maintain Professional Indemnity Insurance coverage. Some of these AISPs and PISPs provide aggregated account access into a much larger community of other third-party providers, which are not themselves overseen by regulators.

In Summer 2025, the government passed the Data Use and Access Act[1] - an historic piece of legislation which laid five foundations for the UK's smart data economy:

1. **Consumer empowerment through data portability.**
2. **Market innovation and competition.**
3. **Trustworthy governance and consent frameworks.**
4. **Sector-specific schemes with regulatory backing.**
5. **Economic growth and public benefit.**

What is smart data? In short, the government wants the Data Use and Access Act to supercharge the UK's economy by stimulating innovation and the creation of new products, services, and markets - driving greater competition and expanding consumer choice. This, in turn, will foster trust and encourage broader participation in the smart data economy, ultimately helping to generate high-value employment and, crucially, attract inward investment. Government estimates smart data will drive a £35 billion increase in the United Kingdom's GDP.[2]

Industry's role Government recognises that industry plays an utterly vital role in the success of smart data; a consistent theme running through the Act is the call to action for industry to build the tools, platforms, and ecosystems that make smart data real. This paper sets out how industry is stepping up to the plate in order to strengthen the smart data ecosystem's defences.

The ecosystem is scaling - but our defences aren't

While the first cohort of the smart data ecosystem, open banking, is expanding rapidly[3], its defences are not yet fully developed – and if the ecosystem continues to scale through open finance to open data without robust, coordinated defences in place, risks will proliferate, cyber criminals will exploit gaps, and the fragile currency of public trust will erode, threatening not just consumer confidence but the legitimacy of the data-driven economy. ***The ecosystem has five key risks:***

Third-party provider impersonation - where a fake app mimics a popular fintech brand, harvesting credentials and potentially enabling unauthorised transfers. This occurred in April 2025 when scammers targeted QuickBooks[4] users by deploying a sophisticated phishing campaign that impersonated Intuit's flagship accounting platform. Fraudsters placed fake ads in Google search results, directing victims to spoofed QuickBooks login pages that replicated Intuit's branding and interface with near-perfect fidelity. Users were prompted to enter their credentials and two-factor authentication codes, which were intercepted using man-in-the-middle phishing kits that could capture this information in real-time.

The phishing domains were designed to closely mimic legitimate QuickBooks URLs. While the campaign successfully harvested user credentials during peak tax season, the full extent of financial damage remains unclear. The sophisticated nature of the attack – targeting business users with access to company bank accounts and payroll systems – raised significant concerns about potential unauthorised transfers and data theft.

Weak consent management - some AISPs have accessed more financial data than users explicitly authorised, often due to vague consent flows or bundled permissions. The World Bank's 2021 Technical Note on open banking consent[5] identified concerns around function creep, namely the gradual broadening or blurring of processing purposes, after a data subject has agreed to the initial collection of the data which may result in unanticipated use of personal data by the controller or by third-parties and in loss of data subject control. The report questioned whether consumers truly understand the scope of access they're granting, querying whether a consumer who consents to a payment service understands and consents to direct access to his or her banking account and whether they realise he or she can limit the consent to access to specific data. And the report warned that when AISPs conflate several purposes for processing and have not attempted to seek separate consent for each purpose, consent is neither free nor informed. The problem is compounded by bundled permissions, where consent becomes a non-negotiable part of terms and conditions making it presumed not to have been freely given. This systematic erosion of user control represents a fundamental flaw in open finance design - access that regulatory frameworks made too easy to give, with inadequate mechanisms to ensure users maintain meaningful control over their financial data.

Mobile app vulnerabilities - an attacker could reverse-engineer a poorly protected app to extract API keys and simulate legitimate requests. In 2023, security researchers from Approov[6] conducted a comprehensive analysis of fintech mobile applications and discovered that 92% of the most popular banking and financial services apps contained easily extractable secrets such as API keys.

The research demonstrated that these hardcoded credentials could be retrieved using standard reverse engineering tools, enabling attackers to impersonate legitimate applications and potentially execute unauthorised API calls against banking systems. This vulnerability is particularly concerning in open banking environments, where such compromised credentials could allow attackers to access customer financial data or perform unauthorised transactions across multiple financial institutions.

Payment redirection & manipulation - fraudsters exploit weaknesses in payment initiation flows – a user could initiate a payment to a known vendor, but malware redirects the payment to a mule account. The Royal United Services Institute's 2025 study on APP fraud[7], flagged fintechs whose infrastructure was exploited by fraudsters using mule accounts and payment redirection tactics. And, in their Annual Fraud Report 2024[8], UK Finance noted that fraudsters are increasingly using malware and spoofed interfaces to redirect payments to mule accounts, even when the user believes they're paying a trusted vendor.

Data breaches & unauthorised access - open ecosystems aggregate sensitive data across multiple platforms, making them attractive targets for data breaches. In 2024, Finastra, a global fintech infrastructure provider used by thousands of banks, was attacked. The criminals exploited stolen credentials to access its Secure File Transfer Platform, exfiltrating ~400GB of sensitive data[9]. While not a breach of open banking APIs per se, the fact that a shared service provider was targeted makes this a cautionary tale for smart data aggregators.

The cost of risk - these five risks are known and understood, but no-one is tracking the full impact. While individual banks and building societies monitor fraud and breaches within their own perimeter, few are tracing incidents back to third-party access via open banking or open finance. As a result, organisations like Cifas[10] lack the visibility to assess third-party provider risk in aggregate. Everyone recognises the risks. Everyone sees them rising as the number of third-party providers proliferates and service usage grows. But without coordinated tracking, the sector remains blind to the financial exposure, reputational fallout, and systemic fragility that third-party failures can unleash.

These risks impact on all five participant groups in the smart data ecosystem.

"If my Exec Team understood that acting now saves money and prevents a data breach, it would be set as a clear priority."

Head of Payments, CMA9 Bank

The victims - who needs to worry and why

Banks and building societies are central to the open finance ecosystem but are concerned about the potential for fraud or data breaches arising from third-party provider access – particularly when factoring in those fourth, fifth and nth party providers that connect into the ecosystem via third-party providers. As such, Financial Institutions worry that they carry the lions' share of liability for fraud and data breach, unsure as to whether a third-party's Professional Indemnity Insurance would cover their cost of remediation. All of which negatively impacts their brand, and has a chilling effect on investment appetite and thus innovation.

"We need to get a handle on this problem before we dive into the Smart Data world..."

Respected Industry Leader

"This should be on the risk register."

Head of Open Banking, UK Bank

"It's not a question of if, but when. Everyone can see this coming. The only choice is whether we act now to close the stable door before the horse bolts..."

Open Banking Lead, UK Bank

"We're like frogs in a pan - we don't know when the heat will reach boiling. While stretched delivering commercial VRP, we recognise the threat, but currently lack the bandwidth to mitigate it."

Open Banking & Digital Platforms, UK Bank

Aggregators act as intermediaries but lack real-time visibility of the risk presented by downstream third-parties, which means they are often blamed when things go wrong, despite having limited control - suffering operational risk, and loss of credibility with banks, building societies and third-party providers. Plus they lack clarity on whether their Professional Indemnity Insurance will cover the real costs of remediation for a bank or building society, let alone the costs of brand damage. Aggregators matter because they are the connective tissue – if they're compromised, data flows fragment and trust across the smart data ecosystem erodes.

"As we scale, our compliance costs rise too. Invela offers a way to contain those costs while boosting operational efficiency."

COO, UK Aggregator

The victims - who needs to worry and why continued

Third-party providers – both regulated and unregulated - span a huge spectrum from long established and well financed to ambitious start-ups with a limited bank balance, and from those connected directly to banks, building societies and aggregators to and those fourth, fifth and nth parties which connect in via third-parties. These providers run the risk of being compromised by malicious actors without always having the depth of experience or pocket to adequately defend themselves – resulting in outcomes ranging from reputational harm to going out of business. Third-parties matter because they're the source of innovation – without a vibrant, growing third-party community, competition stutters.

"Accreditation as an industry trust mark aligns perfectly with our values. We intend to lead the conversation on quality, not just follow it."

CEO, UK Third-Party Provider

Consumers have to manually manage data access revocation when they may have lost track of who holds their data or how it's used, and when they may not be familiar with how to revoke access or be confident that it's worked. And this is also when they have no reasonable way of knowing that a third-party to which they have granted access to their data has been hacked or otherwise compromised. Consumers not only run the risk of financial loss, but also of identity theft and reputational damage, all leading to an erosion of trust and thus a reluctance to share data. Because they're the source of data and the intended beneficiaries, if consumers opt out, the smart data ecosystem simply loses its purpose.

Legislators and regulators are the architects of the smart data ecosystem but are constrained to acting only within their often sector-specific remit, in a world where smart data will increasingly flow across sectors. Meaning that any regulator-led solution would necessarily be a something of a patchwork with both gaps and overlaps, with lengthy implementation timelines and duplicative compliance burdens. In contrast industry-led solutions can be both quicker and less expensive. The Data Use and Access Act lays out the framework for consumer empowerment, market innovation, effective governance, sector-specific schemes, and economic growth. But without industry action, the blueprint remains aspirational.

Case studies

Third-party provider risk: the open finance ecosystem's silent saboteur -

***PayPal's* fraud filter failure and the risk of contagion** - when PayPal's fraud filters failed[11], €10 billion in unauthorised debits flooded European banks exposing a brutal truth: third-party provider risk isn't theoretical, it's systemic. In open finance ecosystems, where openness is the operating principle, a single weak link can trigger contagion. The PayPal breach wasn't just a glitch - it was a governance failure. It showed how opaque, unmonitored third-party provider actions can bypass safeguards and blindside even the most regulated institutions - banks.

***Wealthsimple's* breach and the anatomy of exposure** - when Wealthsimple disclosed a breach[12] affecting thousands of consumers - triggered by a compromised third-party software package - it wasn't just a cautionary tale. It was a live demonstration of systemic risk. The breach was textbook - opaque third-party behaviour, delayed detection, and reactive containment. Government IDs, account numbers, and social insurance data were exposed. Not passwords, but enough to seed identity theft and erode trust. Wealthsimple's transparency was commendable, but the breach had already occurred.

***TransUnion's* exposure and the fragility of trust** - when TransUnion confirmed a breach[13] affecting over four million individuals, it wasn't just a headline. It was a fault line in the foundation of open finance. The breach exposed names, birth dates, and social security numbers — not passwords, but enough to weaponise identity and compromise onboarding across the ecosystem. The anatomy was familiar: delayed detection, limited disclosure, and a sprawling impact. TransUnion's role as a data gatekeeper made the breach systemic. It wasn't just a fintech misstep - it was a core infrastructure failure. Invela calls this the 'credibility collapse': when the institutions tasked with verifying identity become vectors of fraud. The breach didn't just affect consumers. It rippled through lenders, aggregators, and verification APIs. TransUnion's response was measured, but the damage was done. In open finance, trust is the currency - and this breach devalued it.

Smart data is scaling but our defences aren't - fraud and breaches linked to smart data are proliferating, yet remain inconsistently classified, tracked, and reported. This systemic blind spot threatens not just end customer safety, but the credibility and adoption of smart data itself.

The risks and their impact on the participants in the ecosystem present four challenges: **highly distributed opaque risks; unbalanced liability; severely limited visibility into ecosystem health; and a reactive, end customer-led data access revocation model.** The following section explores each challenge in turn and describes how industry can turn it into a strength from which we can scale the smart data ecosystem.

Addressing ecosystem challenges – building strong defences

Ecosystem expansion: from distributed risks to federated resilience

Today, risks are highly distributed and opaque:

Beyond the perimeters of regulation - although 226 third-parties are currently regulated under the open banking scheme[14], thousands of fourth, fifth and nth providers operate entirely legally beyond the perimeter of regulatory oversight. This is because they are not delivering regulated products and services, and use regulated participants (aggregators) for necessary account access. As such the unregulated third parties introduce unknown risks and represent a lack of transparency as to which entities hold consumers' data.

Inconsistent accreditation and no real-time monitoring - no unified standard for accrediting third-parties, other than for those regulated players overseen by the Financial Conduct Authority – and no real-time monitoring of aggregators, third-parties, or those parties beyond the perimeter of regulatory oversight.

Cybercrime blind spots - limited shared intelligence across banks, building societies and aggregators meaning cybercrime patterns go undetected until too late.

Customer vulnerability - retail consumers, businesses, and corporates are unaware of which entities are accessing their accounts, beyond the third-party to which they have granted access.

Operational fragility - without standardised approaches, risk identification, risk management and dispute resolution are slow, manual, and siloed – meaning that poor behaviour proliferates unchecked, undermining the safe expansion of the smart data ecosystem. In turn this restricts the depth, breadth and value of products and services delivered to consumers – to the detriment of both the UK's citizens and businesses, and the economy.

Ecosystem expansion: from distributed risks to federated resilience | Continued

Industry levers to build federated resilience and thus a safer ecosystem:

Standardised, proportional accreditation - starting with open banking, build sector-specific requirements such as consent handing, API standards and certification into accreditation for aggregators and third-party providers. Extend this consistently across the smart data sectors as they come on stream.

Accreditation paired with dynamic real-time risk scoring and monitoring - treat accreditation not as a static badge but as a dynamic object where positively maintained risk scores support continued accreditation, and poor risk scores trigger accreditation reviews.

Real-time alerting – flag negative third-party provider risk score movements to data holders, such as banks and building societies, and to aggregators so that they know when their risk appetites have been breached. As a result, they can take swift, informed action to restrict that third-party's access to data until issues are resolved.

Pooled intelligence – enable the ecosystem to respond faster and more effectively to emerging threats.

Aligned incentives for good governance and proactive risk management - transfer the economic responsibility for risk to those who introduce it to the ecosystem.

Smart data promises many benefits, but without resilience to fraud and data breach and misuse, openness becomes fragility - to unlock the full value of the smart data ecosystem, we must shift from distributed risks to federated resilience: where every third-party provider and aggregator is accredited, risk is continuously monitored, and bad actors are swiftly excluded until issues are resolved. Federated resilience is the foundation for ecosystem expansion, enabling richer products, deeper customer trust, and societal and economic benefit at national scale.

Rebalanced liability: from blank cheque to proportional accountability

Today, liability is unbalanced:

Impact of unbalanced liability - regulators have yet to define a fair, enforceable liability framework across the smart data ecosystem – although the Data Use and Access Act has stressed the need for clear liability frameworks for data misuse and fraud, and the need for transparent redress. Indeed, the FCA's research note[15] on open banking and open finance in the UK called out the lack of a comprehensive liability model as a key weakness. This means that, today, third-party providers introduce risk but aren't always held accountable in a structured way – particularly if unregulated. All of which leaves banks and building societies with worryingly opaque risks and significant liabilities. Scaling the current approach will simply embed unbalanced liability in the smart data ecosystem.

Industry levers to build proportional accountability:

Liability attribution - supported by traceable data points such as entity IDs, risk scores and timestamps to ensure clear accountability.

Seamless, integrated, proportionate liability coverage - where the cost of the risk is born by the ecosystem participant which introduced the risk.

Smart data cannot scale on a liability model that writes blank cheques - today, the ecosystem is unbalanced. We must shift to proportional accountability, where liability is traceable and the cost is born by the party that introduced the risk. This will help to unlock investment and enable the smart data ecosystem to scale safely.

Ecosystem health: from visibility gap to rich insight

Today, ecosystem health is unknown:

Fragmented information - data access and risk exposure are distributed across thousands of participants – with increasing opacity beyond the regulated first tier of third-parties.

Reactive action - banks and building societies act after the fact, and regulators rely on complaints and audits to become aware of issues.

Scaling uncertainty – participants can't assess whether the ecosystem is healthy and worthy of investment, and legislators and regulators can't assess whether the ecosystem is capable of growing safely, equitably, and in line with policy intent.

Industry levers to deliver rich insight into ecosystem health:

Holistic view plus empowered proactivity – where banks and building societies understand which third-parties are accessing consumers' data, the third-party's accreditation status and risk scores, and whether or not there are alerts which flag that that third-party's data access should be restricted until issues are resolved.

Metrics - everything from participant growth numbers; to risk score spectrum, mean and median; to number of alerts per time period.

Only with detailed knowledge of the smart data ecosystem's health can participants and policymakers be confident - without real-time insight into consent flows, access events, and risk exposure, the ecosystem remains opaque - undermining participation, slowing policy momentum, and exposing consumers to systemic risk. Embedding intelligence, automation, and transparency into the core of the smart data ecosystem transforms awareness and action from reactive to proactive. This unlocks confident participation and scalable protection, enabling the smart data ecosystem to grow safely and equitably - and in line with smart data policy vision and ambition. Ecosystem health shouldn't be an afterthought – it must be baked in.

Common sense: from a reactive, end customer-led account access revocation model to a proactive, ecosystem-led model

Today, account access revocation is in the hands of the end customer and thus fragmented:

Revocation fragmentation - when things go wrong, the current system relies in part on end consumers knowing that something has gone wrong; knowing how to manually revoke access to their account; and where to go to do it. Yet this is currently often without any real-time visibility into which entities hold their data, or even whether revocation has been successful.

This fragmented process means consumers may only discover issues once harm has occurred - exposing them to unnecessary risk. In turn this may undermine their confidence in their bank or building society and in using their data to power personalised products and services. And it may leave them to deal with lengthy and bureaucratic processes to put right the loss that they have experienced.

Industry lever to build a proactive, ecosystem-led model for account access revocation:

Ecosystem intelligence - dynamic risk scores trigger automated account access revocation alerts for banks, building societies and aggregators, enabling them to act as soon as they have evidence of potential harm, before consumers are affected en masse.

Smart data access revocation shouldn't rely on consumer vigilance and competence, it should be built into the system - shifting the account access revocation burden from fragmented, manual actions performed by consumers to a real-time, ecosystem-led model transforms account access into a trust-enabling function. Banks, building societies and aggregators - positioned at the nexus of data exchange - can revoke account access swiftly, based on real-time data-driven risk signals. This model reduces exposure to fraud, breach and other risks, and builds ecosystem integrity and resilience - unlocking smart data's full potential, while supporting and enabling smart data principles of portability, transparency, and control.

Open Finance Risk Management: Invela's three lines of defence

Having explored each challenge in turn and described how industry can turn challenges into strengths from which we can scale the smart data ecosystem, the final section of this paper describes how Invela's three lines of defence federate trust, rebalance liability, build healthy smart data ecosystems, and enable proactive, system-led account access revocation – and the value that this brings to each participant in the ecosystem.

Invela Accrediation - Our first line of defence is a detailed, sector-specific accreditation (and, at a minimum, annual re-accreditation) process for aggregators and third-party providers delivering effective vetting and ongoing risk management of the smart data ecosystem. Developed and delivered with a globally recognised and trusted ratings partner, this accreditation complements the processes run by the Financial Conduct Authority and Open Banking Ltd, and it extends beyond those processes to cover the unregulated part of the ecosystem. Once accredited, the aggregator or third-party joins the Invela Network.

Invela Risk Score Indicator - Our second line of defence is entity-level risk scoring based on behaviour and a very large number of different data sources, not just status at accreditation. Banks, building societies and aggregators are provided with real time alerts, flagging (when that provider breaches their individual risk appetite) that they should consider revoking a third-party provider's access.

Invela Warranty - Our third line of defence is an efficient risk transfer framework which compensates data holders when losses occur, informed by Invela's Accreditation and Risk Score Indicator.

Governance - the Invela Network is governed by transparent, non-discriminatory accreditation and risk protocols, ensuring fair market participation without exclusionary practices.

Invela's value

Banks & building societies move from blind exposure to intelligent stewardship - Invela restores banks and buildings societies' control, transforming opaque risk visibility into actionable intelligence, enabling institutions to manage aggregator and third-party data access with precision and confidence, increasing operational efficiency and reducing exposure to data breach, misuse and fraud - and thus the associated financial cost and reputational impact.

Aggregators move from conduits to valued gateways - aggregators are the connective tissue of the smart data ecosystem - but without the right tools, they're exposed to risk without sufficient control. Invela flips that dynamic, empowering aggregators with dynamic real-time alerts flagging downstream exposure, allowing them to act decisively to reduce risk for banks and building societies – while increasing their operational efficiency and building trust across the ecosystem.

Third-party providers move from opaque risk to trusted participants – the extended third-party network, encompassing fourth, fifth and nth parties, are the innovation engine of the ecosystem. Invela's detailed accreditation, real-time risk scoring and risk transfer mechanisms enable these providers to actively reduce the risk they present to the ecosystem – while increasing their operational efficiency and building trust with aggregators, banks and building societies.

Consumers benefit from frictionless protection and empowered participation - Invela's infrastructure delivers real-time protection by enabling bad actors to be excluded by banks, building societies and aggregators when issues occur, protecting consumers from financial loss and reputational damage. As consumers are both the source of data and the intended beneficiaries of products and services powered by their data, this reinforces the smart data virtuous circle of engagement and innovation.

Invela is delivering the smart data ecosystem's multi-layered, intelligence-driven defence infrastructure, transforming smart data risk management from static compliance into dynamic, real-time resilience – protecting both participants and consumers from breach, fraud, and data misuse. By integrating accreditation, risk scoring, and real-time alerts with a risk transfer framework which compensates data holders when losses occur, Invela doesn't just detect risk – Invela incentivises better performance, aligns participant accountability, and creates a self-reinforcing smart data ecosystem built on transparency and trust.

Call to action

Industry is stepping up to the plate. Invela is delivering a simple, elegant solution.

Open Finance Risk Management

The call to action is clear - smart data cannot scale on risk opacity and unbalanced liability. It must be underpinned by fairly distributed accountability and aligned incentives - only then can it transform from an incentives lottery and liability minefield into a safe, resilient and scalable smart data ecosystem where consumers benefit from frictionless protection and empowered participation.

Industry is stepping up to the plate; Invela is delivering a simple, elegant solution – Open Finance Risk Management - to help the smart data ecosystem scale safely and thus to realise the ambitions of the Data Use and Access Act.

Citations

[1]Data (Use and Access) Act 2025

[2]Data use and access bill regulatory powers for smart data impact assessment

[3]https://www.openbanking.org.uk/news/open-banking-surges-to-15-million-uk-users-as-july-marks-record-adoption/

[4]Tax deadline threat: QuickBooks phishing scam exploits Google Ads | Malwarebytes

[5]World Bank Document

[6]Approov Secrets Report v1.0.1.pdf

[7]Following the Fraud: The Role of Money Mules | Royal United Services Institute

[8]Annual Fraud Report 2024 | Policy and Guidance | UK Finance

[9]Fintech giant Finastra confirms it's investigating a data breach | TechCrunch

[10]https://www.cifas.org.uk/

[11]European banks hit by rogue PayPal payments worth 'billions' - BBC News

[12]https://www.finextra.com/newsarticle/46562/wealthsimple-data-breach-exposes-customer-information?utm_medium=newsflash&utm_source=2025-9-9&member=36853

[13]TransUnion Breach Impacts 4.4 Million — How to See If You're at Risk

[14]Directory Archive - Open Banking

[15] Research Note: Open banking and open finance in the UK | FCA