It Takes a Village

How United Data Stops Organised Fraudsters

An Experian Perspective

Authors

Jon-Marius Bru - Presales Consultant, Experian Northern Europe
Jakob Færgeman - Global Consultant, Experian Northern Europe

The Village and the Fraudulent Knock at the Door

Lending and trust are not new inventions; they’re older than ancient Nordic villages.

Long before digital banking or identity checks, communities thrived on shared reputation, word of mouth, and the simple integrity of a person's word. In these close-knit settlements, a loan was more than a transaction – it was a testament to mutual faith.

One evening, Askr knocked on doors asking for a small loan to help his family. Each household takes his word and trusts that he will pay them back, since he promises them that the times he has borrowed money, he has paid it back. Yet, unbeknownst to them, he is visiting every house with the same story. Individually, each villager lends him a small sum, not realising they’re all being duped. However, in one town meeting, someone mentions that Askr hasn't paid them back for several months. Each household stands up one by one to complain about the same, but Askr is nowhere to be found.

Banks and lenders can find themselves in this very scenario in today's digital world. A loan application arrives and looks legitimate on paper. They have a strong credit score and no red flags, but the applicant is a fraudster wielding a stolen BankID and a hijacked shell company as cover.

The fraudster knocks on the doors of many banks, trying to exploit the fact that no single institution can see the full pattern of his activities. Like the villagers, it takes a united community to spot the fraud: if the banks shared their "visitors' behaviours", they would quickly realise the same person is trying to defraud them all.

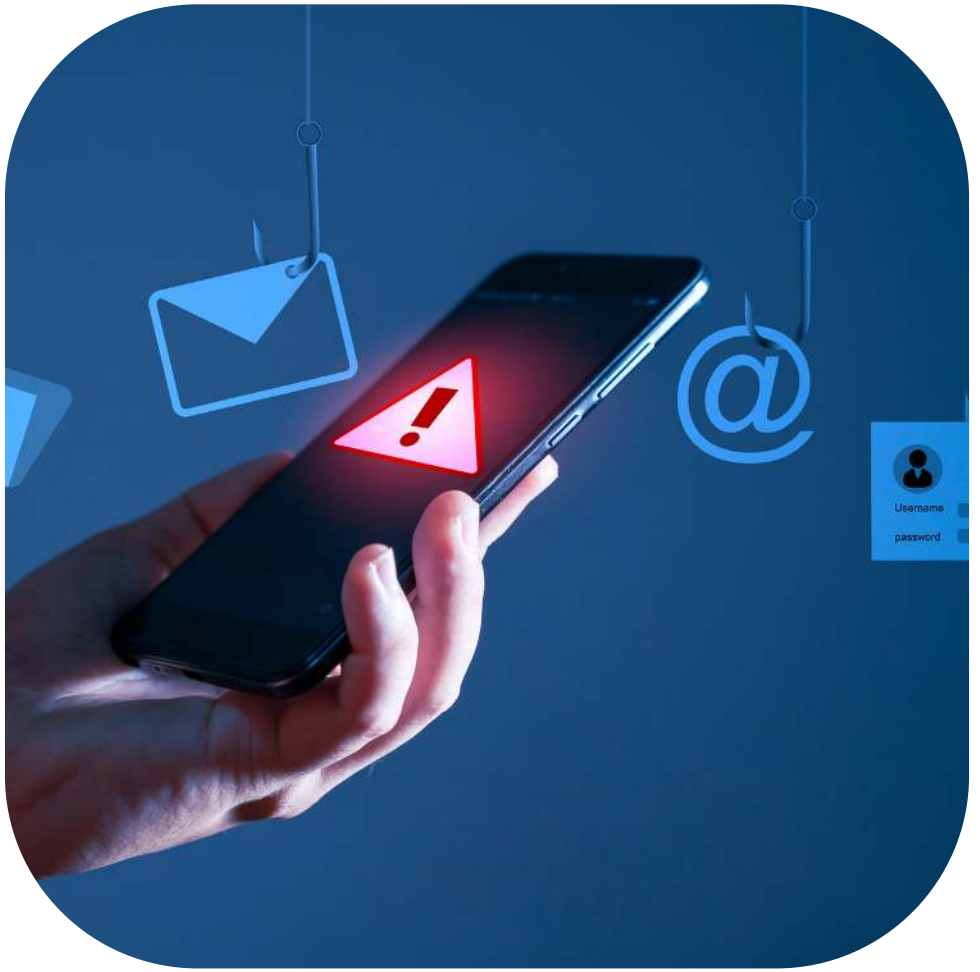
This white paper shows why Norwegian financial institutions must now join forces to stop highly organised, modern fraud schemes actively.

The Problem – Smarter Fraud in a Village Without a Watchtower

In Norway and Denmark, consumers enjoy some of the world's strongest digital ID systems (BankID, NemID/MitID). These national e-ID schemes make it hard to fabricate a completely fake person, since synthetic identities are nearly impossible when every loan applicant must authenticate with an industry-standard digital identity verified by official government data. One might assume this security would end identity fraud. Yet, determined fraud rings have adapted: rather than inventing fake people, they steal or hijack real ones.

We see criminal syndicates phishing these e-ID credentials, taking over dormant companies' registrations and combining bits of real data to create "synthetic business identities". They "employ" unaware consumers and update public registries and tax reports with fake information. In other words, they exploit the trust in real identities and businesses to slip through undetected.

Modern fraud is no longer the realm of isolated "lone wolf" scammers. It has become industrialised and organised, often by cross-border rings using advanced technology. According to Experian's latest fraud research, there's been a clear shift "from individual fraudsters to highly organised fraud syndicates," a trend accelerated by the advent of generative AI. Generative AI (GenAI) tools now enable criminals to create persuasive fake documents and even "deepfake" identities to progress through verification checks.



Fraudsters armed with GenAI can scale up their attacks dramatically – one report notes that GenAI has "changed the fraud landscape forever," allowing crooks to churn out synthetic IDs and deepfakes easily and without the restrictions regulators impose. A single fraud ring can simultaneously impersonate numerous people and businesses with uncanny realism.

The fauxface of GenAI

Norwegian Bank, DNB, recently shared a story where fraudsters impersonated their CFO and CEO with GenAI in a video meeting, trying to get unlawful access to funds.

Norwegian banks have seen growing incidents of such advanced impersonation. For example, a fraudster may use a deepfake video chat to “prove” their identity or hijack a dormant company by changing its registration info, then apply for credit in the company’s name. There have been media reports where an entire company was stolen and exploited while the founder was on annual leave!

The scale of the threat is growing. Over 54% of businesses worldwide report an increase in fraud losses in the past year, even in regions with strong ID systems. Fraudsters are using new techniques like synthetic business identities and account takeovers of real customers.

In Norway, officials note an “increased use of social engineering” – criminals calling victims pretending to be banks or police to trick them into divulging BankID codes or transferring funds to “safe” accounts. In other words, even when the front door (BankID) is secure, fraudsters find a side window – human gullibility or procedural gaps – to climb through. The result is a cat-and-mouse game: as soon as one fraud method is blocked, another arises. Generative AI has supercharged this cycle by lowering the skill needed to execute complex and sophisticated fraud.

Crucially, organised fraud rings exploit the lack of collective visibility among institutions. Each bank on its own sees only a slice of the attack, for example, a single fraudulent loan or credit card application, which might go undetected in isolation. Fraudulent patterns only appear when looking across institutions. For instance, one bank might see a loan applicant using an address that, at another bank, was recently flagged in a money mule case; or multiple banks might see loan requests from different individuals, but with the same IP address or device fingerprint. Only by pooling these clues can we reveal the fraud network at work. Experian’s 2024 Global Fraud Report highlights that businesses typically only see their “on-us” data, but wider data sharing exposes "off-us" patterns that no single lender can catch.

This is especially pertinent in the Nordics: strong IDs make outright fake identities rare, but that pushes fraudsters to reuse bits of real identities across many targets – a pattern that only a shared data view can detect.

It's also worth noting that today's financial fraud is not a victimless crime. Often, the proceeds fund organised crime networks well beyond the fraud itself. Law enforcement and Europol have found that gangs engaged in credit fraud and identity theft funnel that money into everything from drug trafficking to terrorism financing. For example, segments of Russian and Eurasian organised crime are heavily involved in financial fraud (credit card and online banking fraud) as a core business, using those illicit profits to fuel other criminal enterprises. This means a fraudulent loan in Oslo might indirectly be financing narcotics or cybercrime operations abroad. Such realities raise the stakes for fraud prevention – stopping a fraudulent loan isn't just about preventing a write-off, it's about cutting off criminal revenue streams.

The problem facing Norwegian and Danish financial institutions is a paradox. They operate in a region of very high trust and strong digital identity, yet they are under attack by highly sophisticated, globally organised fraudsters who abuse that trust. GenAI-driven fake identities, deepfakes, social engineering, and coordinated multi-bank attacks have made fraud harder to spot using traditional, siloed defences. The good news is that the core Nordic ethos of cooperation might hold the answer, turning that village feeling into a modern, data-driven defence. Just as rowers move fastest when perfectly synchronised, Nordic institutions can outpace sophisticated fraud by pulling together through shared data and unified defences.

A Digital Neighbourhood Watch through Consortium Data

How can banks and lenders band together like a vigilant village? The solution gaining momentum is the concept of fraud data consortia – essentially a "digital neighbourhood watch" for financial fraud.

In a fraud consortium, multiple institutions securely share fraud signals and data in real time. If one member of the consortium meets a suspicious application or transaction, the others get an alert (or can query the data) before they too fall victim. It's as if one house in the village yelled out a warning about the con artist at the door so that the neighbours could bolt their locks. This collective intelligence approach is not theoretical – it's already proving effective in other markets. Industry experts are emphatic that collaborative data sharing is now essential. In fact, 83% of fraud leaders in Norway, agree that it's crucial for external institutions to collaborate for effective fraud prevention. Likewise, a global survey found that nearly four out of five fraud decision-makers say that external collaboration is key to combating fraud.

> In today's threat landscape, if you're not in a consortium, you're playing blindfolded. A single bank's data tells a story. A fraud consortium tells the whole plot, and that's how you stay ahead of the criminals.

So, what does a fraud consortium look like in practice?

One model is Experian's National Fraud Prevention Solution (NFPS), used in the UK and Europe, as well as globally (US, India, Brazil), which functions as a cross-industry or a single industry fraud network. Every new credit application a member bank receives is automatically checked against the consortium's shared database of confirmed frauds and suspicious patterns. The idea of the NFPS is to highlight suspicious applications, allowing you to investigate and prevent fraud without inconveniencing genuine customers.

In other words, it's innovative and real-time – if fraudsters try the same stolen ID at Bank A, then Bank B, those attempts leave a trail that the next bank can detect and stop instantly. Consumers may be shopping for the best offer and thus have applied for a loan with multiple banks. The key here is to spot the clues that distinguish the suspicious applications from the real applications. This is far superior to the old way of discovering fraud after losses occur (through police reports or insurance claims). Instead of retrospective alerts, consortium data allows proactive blocking.

For example, if a fraudster applies for a loan at DNB with a stolen identity and triggers a warning in the consortium (say, because that ID was used at Nordea an hour before), DNB can pause or decline the application before disbursing funds.

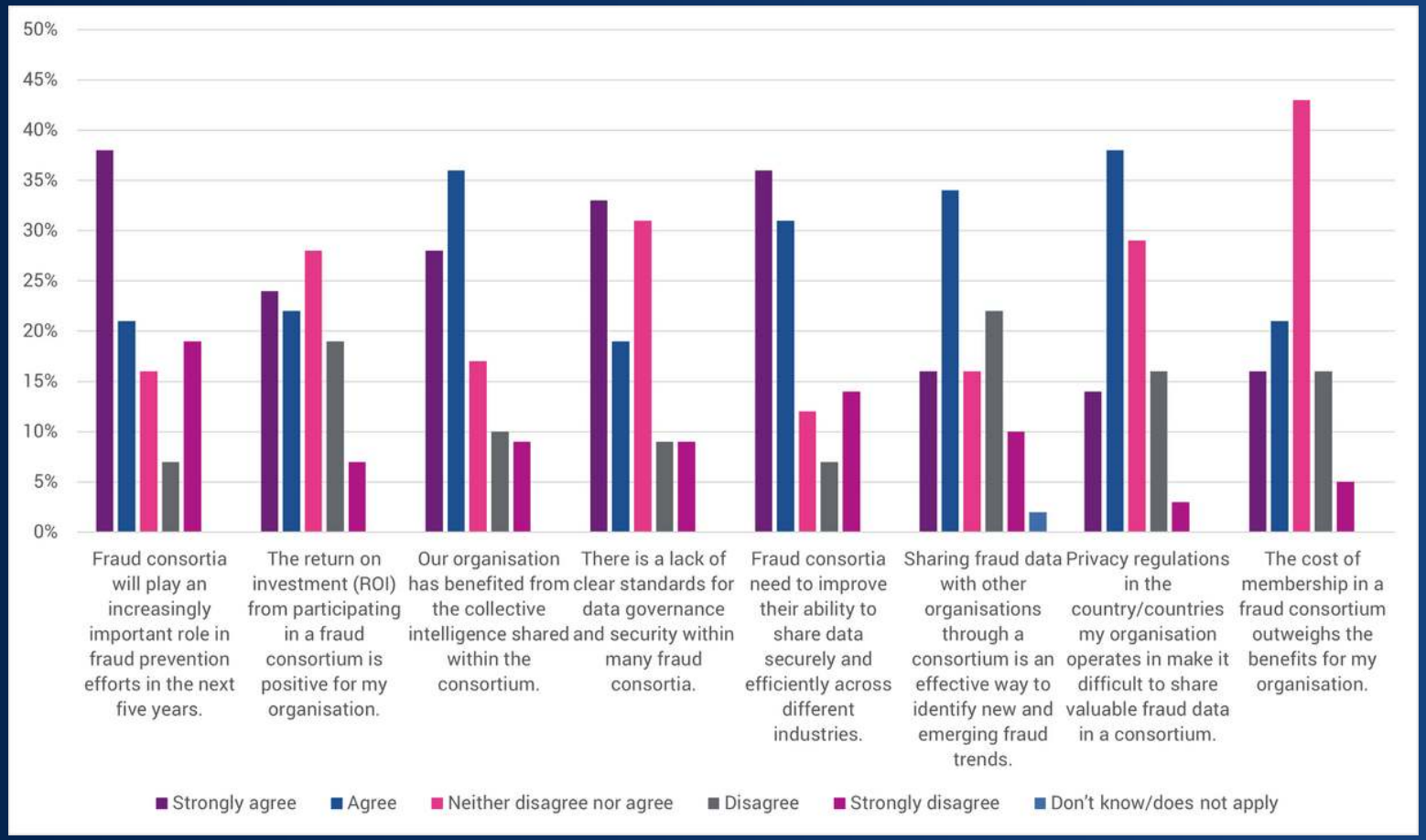
It's a real-time "license plate check" for fraud: much like police running a plate number to see if a car is stolen, a bank can run an application's details through the consortium. A positive "hit" doesn't automatically accuse the customer of fraud (just as a flagged license plate doesn't immediately jail the driver); rather, it signals "proceed with caution" and prompts further verification. This ensures innocent customers aren't unjustly harmed, while dramatically raising the bar for fraudsters. As with the license plate, an identity might be stolen and used by someone else. Like the police check the license plate and see that it belongs to a BMW but is now used on an Audi, suspicion can also be raised with an identity, and further controls should be done not only to stop the criminal but to protect the owner of the identity.

Collaboration via consortia is essentially an orchestrated defence. Instead of each bank relying on its limited data, members pool their intelligence. Fraud patterns that would be invisible in one dataset become starkly apparent across a network. Advanced consortium platforms integrate seamlessly with other fraud tools (device fingerprinting, behavioural biometrics, etc.) as part of a layered defence. This fraud orchestration means all signals – both internal and shared – feed into one decision engine in real time. The result is a higher fraud catch rate with minimal added friction for legitimate customers. Experian's research shows that fraud orchestration platforms are becoming essential to juggle multiple fraud tools effectively. A consortium is a critical piece of that puzzle – it's an extra "sensor" that can catch what in-house tools might miss.

Importantly, consortium data sharing is gaining acceptance and delivering ROI. A recent global survey of fraud executives found that 63% agree that sharing fraud data through a consortium helps identify new and emerging fraud trends. Even more compelling, 64% of businesses have seen a positive return on investment from taking part in a fraud consortium. This success is why 62% of organisations globally believe fraud consortia will play an increasingly critical role in the next five years. The concept of a shared fraud database is quickly moving from a nice-to-have to a must-have in the toolkit.
How does Norway compare? Thus far, the Nordics have used collaboration mainly in informal information exchanges and joint task forces (for example, the Nordic Financial CERT for sharing cyber threat intel). A dedicated fraud data consortium for banking isn't yet as prevalent in Norway as in the UK, but interest is rising, and we even see the FSA arranging a regulatory sandbox project to evaluate initiatives.

To understand how Norwegian organisations view the future of fraud data sharing, we asked 58 business leaders to weigh in on their experience and expectations with fraud consortia. Their responses paint a clear picture: optimism is growing, but concerns still need to be addressed to unlock full participation.

What Norwegian business leaders are saying



The results above reveal a pivotal moment for the Nordic fraud prevention ecosystem. Business leaders believe in the power of shared data – but legal clarity, trust frameworks, and practical tools will be key to turning belief into action. If we build the right infrastructure, the willingness to collaborate is already there.

Legal Hurdles, Cultural Hesitation, and Risk

If fraud data sharing is so effective, why isn't everyone doing it already? The answer lies in legal, cultural and risk barriers that have made institutions cautious. Data privacy laws like GDPR and Norway's Personal Data Act (Personopplysningsloven) are foremost. Banks are understandably nervous about sharing customer information, even fraud-related information, for fear of violating strict privacy regulations.

Fintech companies are equally, if not more, cautious about this topic, afraid of not being compliant, and they play it safe with regulations. The concern is that by pooling data, they might inadvertently expose personal details or violate consent rules.

There's also the potential ambiguity in how regulators interpret such data sharing: is it a "legitimate interest" for fraud prevention (which GDPR does allow to some extent), or could it be seen as using data for a new purpose beyond the original scope? Lacking explicit guidelines, many compliance officers default to caution.

As one survey finding noted, over half of organisations feel there are no clear standards for data governance and security in fraud consortia they could join. This uncertainty feeds a chicken-and-egg problem – without clear standards or precedents, each institution hesitates to be the first mover.

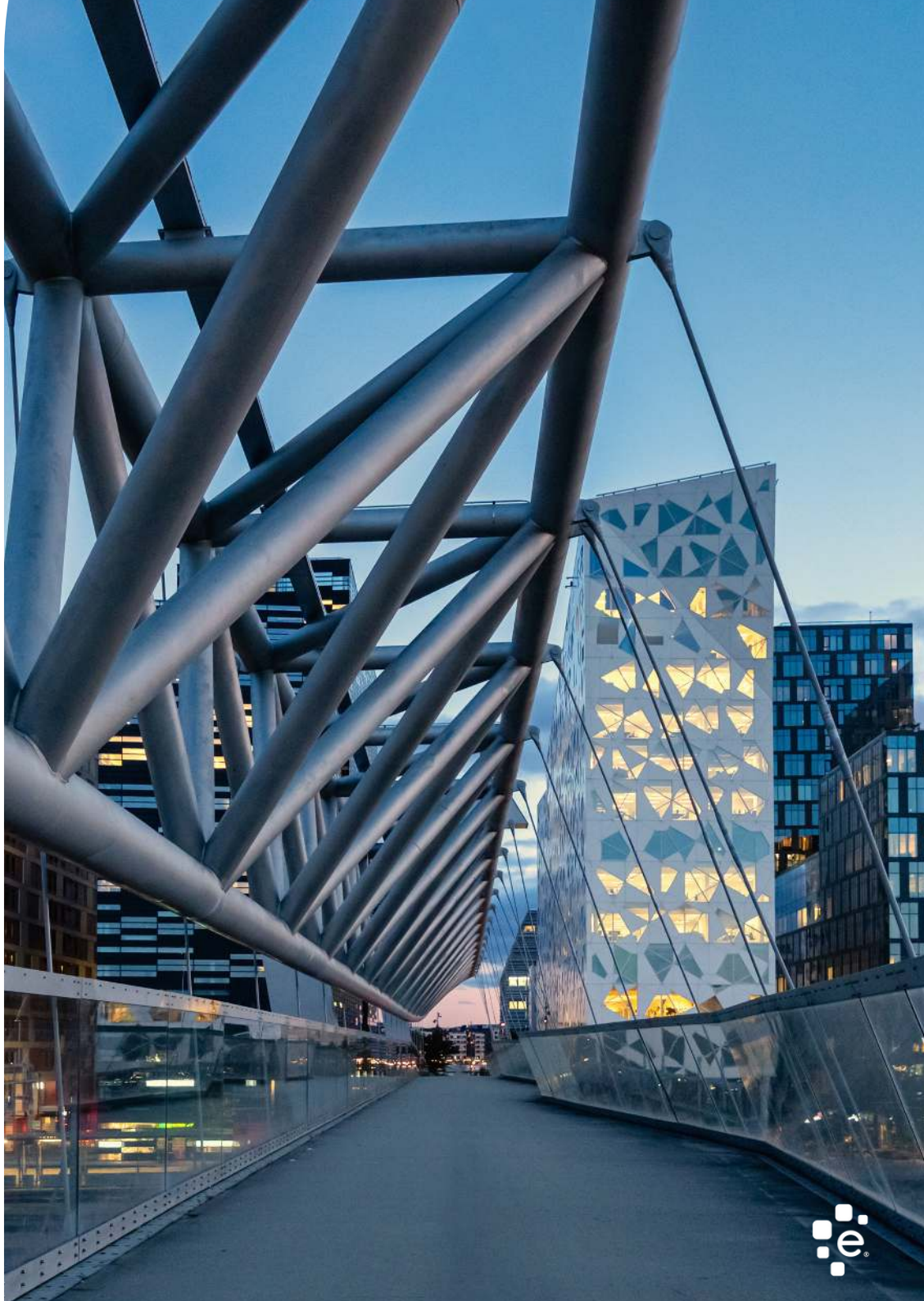
Another barrier is the fear of overstepping or liability. Some financial institutions worry that if they contribute data which labels an individual as suspicious, but the individual is innocent, they could face legal repercussions. It's a bit like the village neighbours being afraid to report a suspicious person in the area in case it's a misunderstanding and they get punished for defamation? A well-run consortium uses controlled, probabilistic alerts – flagging patterns, not publicly blacklisting customers. It's about sharing intelligence (often anonymised or coded), not definitive judgments. The "license plate check" analogy applies: a consortium alert is an advisory for further investigation, not an outright ban on a person. Nevertheless, getting comfortable with this distinction takes time. Banks also voice concerns about governance: who runs the consortium, who has access to the data, and how to ensure it's used only for fraud prevention and not for competitive insights, etc. Without a strong governance framework, some banks won't join due to reputational risk.

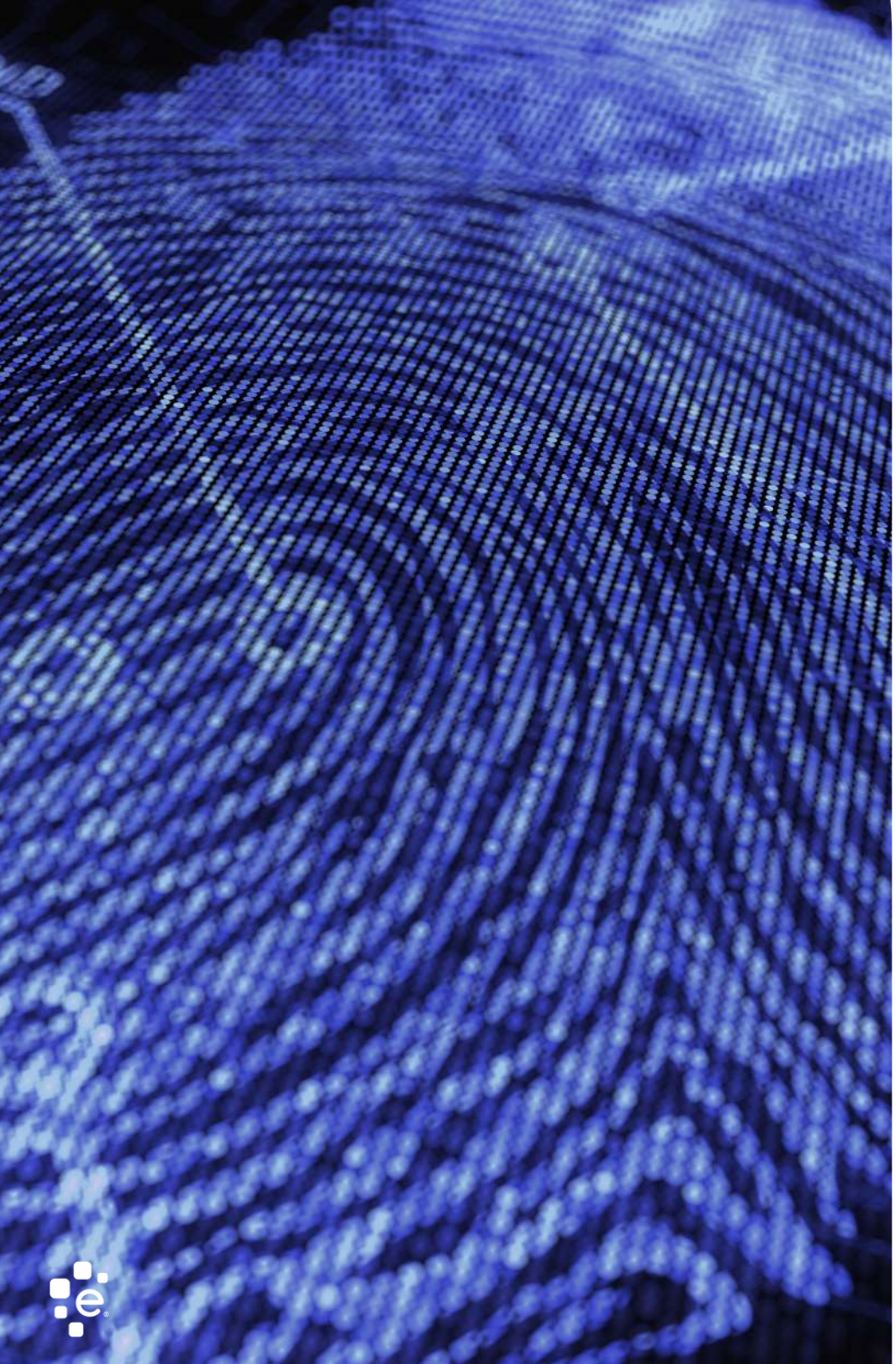
Regulatory interpretation is gradually catching up. Notably, some countries have clarified or even mandated fraud-data sharing in the public interest. For example, Brazil endorsed a regulation (the Central Bank Resolution No. 6), which makes it compulsory for financial institutions to share information that indicates fraud with each other. The UK, while not mandated by law, strongly expects firms to take part in intelligence-sharing to prevent fraud at a systemic level. These examples provide a helpful contrast: they show that privacy and data sharing can be balanced with the proper legal framework.

> Collaboration doesn't mean compromising privacy, it means putting the right safeguards around shared risk.

There is also a cultural factor: historically, banks have been reluctant to share information with competitors. In a highly competitive market, the idea of sharing even fraud data can trigger fears of losing an edge or exposing one's own weaknesses. However, this mindset is slowly changing as the industry recognises that fraud is a shared enemy. Fraudsters are, in fact, counting on banks' unwillingness to talk to each other. Every gap between siloed defences is an opportunity for criminals to exploit. The "village" must realise that collaboration on fraud does not undermine competitive position – if anything, it protects the whole financial ecosystem (and public trust in it). In our metaphor, one house spreading the word about a scammer doesn't lose anything; it helps ensure the whole neighbourhood is safe, which helps everyone.

Credit risk is another critical area where collaboration already plays a trusted role. Just as fraud prevention depends on shared signals, responsible lending relies on shared credit data to protect consumers from overextending themselves. In Norway, lenders use credit remarks, shared via credit bureaus, as early warnings of financial distress. These data points help ensure that no one bank unknowingly lends to someone already in default elsewhere. This is a clear example of regulated, privacy-conscious data sharing already working in the consumer's interest. A fraud consortium would simply extend the same logic: not just protecting people from borrowing beyond their means, but from having someone else borrow in their name. In both cases, data sharing isn't a risk; it's a safeguard.





Overcoming these barriers will require a combination of clarifying the legal ground rules and building trust through proven governance. Clear guidelines (perhaps an industry standard or regulator-approved code of conduct) for consortia can assure banks that “if you do X, Y, Z safeguards, you are compliant.” For example, ensuring that data isn’t shared unless there is a suspicious match, limiting data to be shared to strictly fraud-related fields, and only used to identify fraud risk.

Essentially, consortia should work on a “need-to-know” principle akin to anti-money laundering exchanges, where specific data can be shared under defined conditions without breaching privacy law. The technology exists to do this in a privacy-conscious way. Again, if we compare this to Norway credit bureau data, this can be managed in the same way. If the application or transaction doesn’t give a match, no alert is provided, and nothing is shared.

These legal, liability, cultural and risk hurdles are real but not insurmountable. Other countries are showing that smart regulatory support can unlock industry data sharing.

Within Norway, there’s a growing realisation that not sharing fraud data may ironically put consumers at greater risk (because organised fraud goes unchecked).

The Opportunity – Stronger Together for Proactive Protection

If institutions can navigate these barriers, the upside of consortium-based fraud prevention is enormous. Primarily, real-time data sharing enables predictive insights rather than reactive damage control. Instead of investigating fraud after customers have already been victimised, banks can intercept attempts at the point of application or transaction. By pooling data, banks collectively build a richer picture of emerging fraud methods. Patterns that one bank alone might write off as an anomaly can be recognised as part of a trend when seen across many data points. This leads to earlier warnings – akin to an epidemic intelligence network spotting the first signs of a new disease outbreak and stopping it from spreading. In the fraud context, one bank's encounter with a stolen identity can alert all consortium members to tighten scrutiny on biometric checks before the wave hits them. Such proactive defence is vital when criminals are using tools like GenAI to morph their tactics constantly.

Another significant opportunity is using AI and machine learning (ML) on top of consortium data to orchestrate faster and more accurate decisions. With a broad data canvas, advanced ML models can draw connections that humans might miss. Imagine an AI-driven system that, as soon as an application comes in, checks dozens of features: Is the email domain one that's been associated with fraud elsewhere? Is the national ID number appearing in multiple banks' recent queries? Is the device used consistent with the genuine owner's prior behaviour, or does it resemble devices seen in fraud rings?

All these checks can happen in a blink, yielding a risk score that can inform the lender's decision in real time. This kind of live orchestration across multiple data sources drastically reduces false positives as well. Why? Because decisions are more informed. A customer who might look risky in one bank's silo (perhaps due to a mismatched detail) could be verified as trustworthy through corroborating data from others. Conversely, a crafty fraudster who might have sneaked under the radar of one bank's rules can be unmasked by a consortium signal that flags, for example, "this ID was used in three loan apps this week." Fewer false positives mean less friction for legitimate customers – an essential goal in an era when consumers expect fast, hassle-free digital service. Indeed, studies highlight that better data integration leads to fewer false fraud flags and a better-quality customer experience.

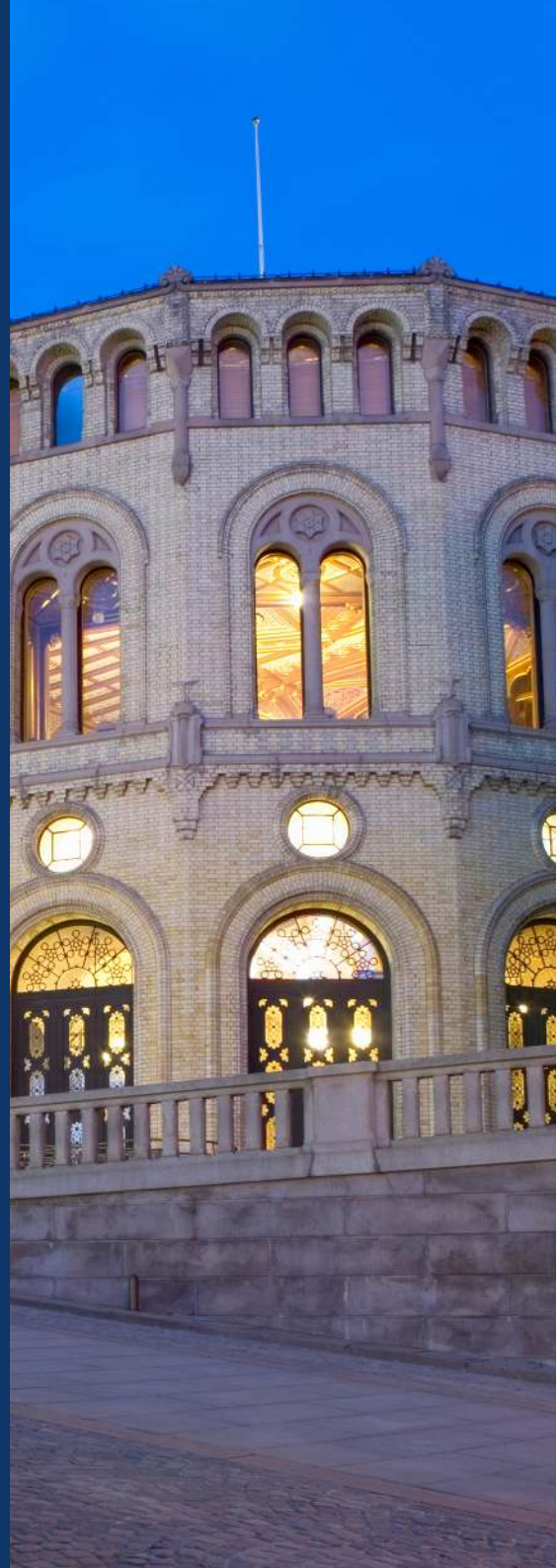
From a customer protection standpoint, consortium approaches significantly reduce the impact of identity theft on victims. If a customer's personal info is stolen, consortium alerts can prevent fraudsters from successfully using that info at multiple institutions. This not only saves the bank money but also spares the customer the nightmare of resolving multiple fraud accounts. It's a win for consumer trust: people know that if their bank is part of a coalition, there's an extra "net" to catch misuse of their identity anywhere in that network. In a region that highly values consumer safety, this added protection reinforces confidence in digital banking. It's worth noting that in Norway's case, truly synthetic identities are rare (thanks to BankID), so most ID fraud involves real people's stolen details. Sharing fraud outcomes, for example, "ID number X was used fraudulently", helps protect those real people by quickly alerting all banks that try under that ID are likely not genuine. It essentially vaccinates the system against further abuse of that identity.

Of course, any such data sharing must be done responsibly and securely. But modern technology provides tools to do exactly that – from encryption to secure multiparty computation – ensuring that even shared data can remain confidential and only be used for its intended purpose. The opportunity, therefore, is to design consortium platforms that bake in privacy by design (so banks can comfortably take part), while delivering the collective insight that yields powerful results. Experience from other countries shows that technical platforms that exist have granular controls: participants only see what they need to for a match (e.g. a reference ID for a prior fraud case), and strict rules govern access. By implementing similar or even more advanced controls, Norwegian consortium initiatives can address privacy concerns and reap the benefits of sharing. Essentially, we can have both security and collaboration – they are not mutually exclusive.

Consortium Use & Adoption Plans

When asked about data consortia use and adoption, 58 Norwegian business leaders indicated:

- 24% currently use some kind of data consortia
- 50% plan to invest in data consortia the next 12 months
- 26% have no plans to invest in data consortia



A Call to Arms for Community Defence

"Does our current interpretation of privacy laws truly protect consumers – or does it inadvertently shield the fraudsters?"

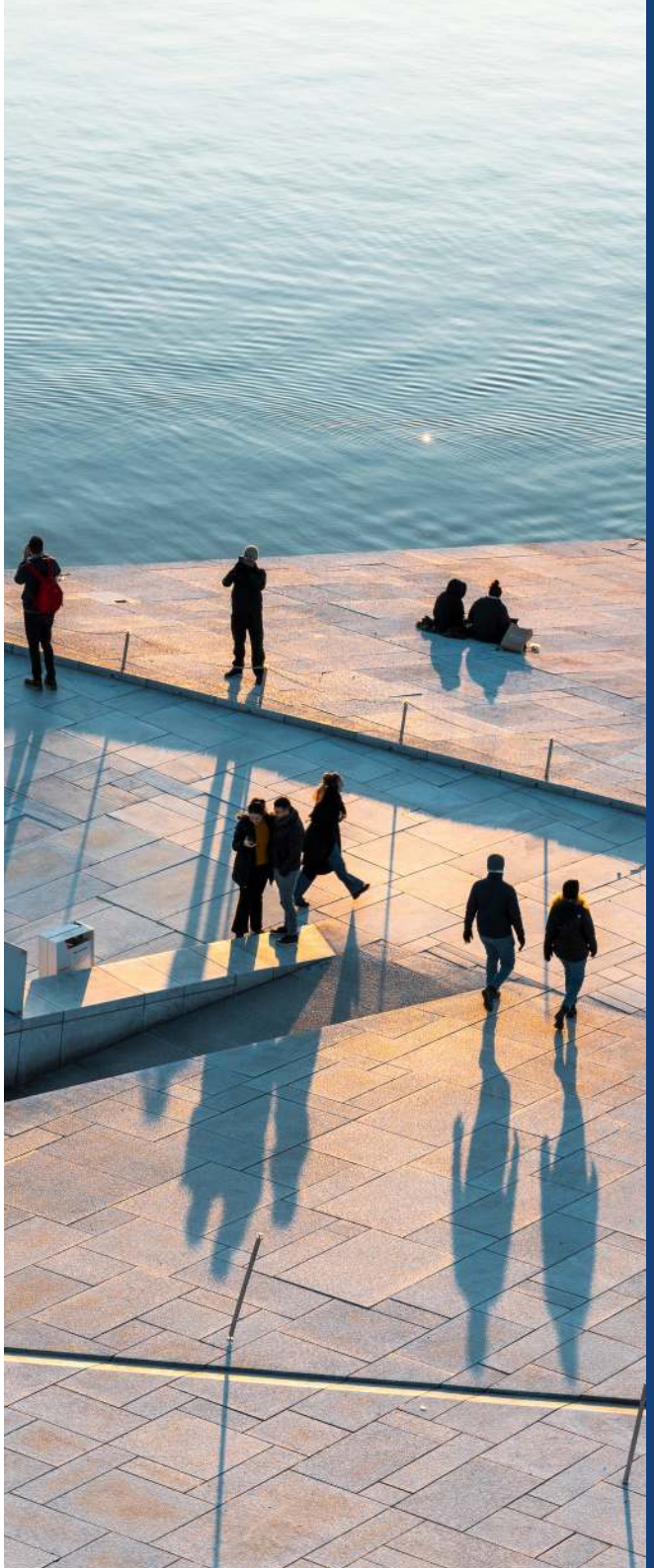
This provocative question should be at the forefront of the minds of regulators and industry leaders alike in Norway. The status quo, where banks fight fraud primarily in isolation, is increasingly untenable against organised syndicates that work without such constraints. Paradoxically, clinging too tightly to siloed data in the name of privacy may enable more consumer harm by giving criminals dark corners to exploit undetected data. It's time to challenge this status quo. The Nordic financial industry, regulators, and policymakers need to collaborate more boldly to strike the right balance.

This does not mean discarding privacy – far from it. It means recognising that smart, controlled, and limited data sharing for fraud prevention serves the public interest and can be done in a targeted, legally sound way. Think of the "license plate" concept: allowing banks to flag suspect identities or patterns to each other is akin to police sharing criminal license plates – it doesn't broadcast personal data to the world; it simply alerts those who need to know. Such alerts protect consumers from having their identities abused repeatedly.

The authors of this paper ask you: if a criminal is using your stolen ID across ten lenders, would you not prefer that those lenders warn each other and stop it early? The answer is obvious – of course you would!

Regulators in Norway and Denmark should consider giving more explicit guidance or frameworks to encourage consortium models. The village mindset – where an attack on one member is seen as an attack on all, prompting a coordinated response, is the only adequate response in this new era of fraud. Experian's fraud survey shows overwhelming agreement on this point: 78% of fraud leaders say collaboration with external partners is crucial to fight fraud. The will is there; now it needs the structure and permission to act.

In practical terms, forming or joining a fraud consortium should become a strategic priority for financial institutions' fraud prevention in the coming year. Executives and compliance officers can start with pilot projects – sharing non-personal risk markers or blacklists – and gradually expand as comfort and trust build. Early successes will show the value (and there will be successes; recall that most participants elsewhere saw positive ROI). Each prevented fraud that would have slipped through without consortium data is proof that united data makes a difference.



Those proof points will also help engage regulators in an evidence-based dialogue about updating any laws or rules that pose unnecessary obstacles.

Ultimately, the fight against organised, technology-boosted fraud is asymmetrical if we stay divided – the fraudsters coordinate, and we do not. Turning the tables requires convergence of data, of tools, and of institutions. This white paper has argued that a community defence – an alliance of banks using shared intelligence – is not just ideal but imperative. The Nordics have a proud tradition of community and trust; by extending that ethos into the digital realm of fraud prevention, they can protect consumers even better than before.

It indeed "takes a village to stop a thief." In the face of AI-enabled fraud cartels, our only choice is to build a bigger, smarter village. By sharing the correct data in the right way, financial institutions can collectively shine a light on fraudsters who once lurked in the shadows between them. The village doors are now bolted, the watchtower is manned, and the alarm bell is ready to ring – all that remains is for everyone to agree that when the next fraudster comes knocking, we ring it together.

References

1. Criipto (2023). Preventing Identity Fraud Online: Norway Interview. Available at: https://www.criipto.com/blog/how-to-prevent-online-identity-fraud.
2. Europol & FBI Reports (2018). Organised Crime and Fraud. Available via FAU:https://business.fau.edu/centers/center-for-forensic-accounting/public-resources-on-fraud/particular-areas-of-fraud/organized-crime-and-fraud/.
3. Experian (2024). 2024 Future of Fraud Forecast. Available here: https://www.experian.com/blogs/insights/fraud-trends-2024-experians-future-of-fraud-forecast/
4. Experian (2024). Global Insights 2025 Predictions. Available here: https://www.experian.com/thought-leadership/business/global-insights-2025-predictions
5. Experian (2024). Redefining Risk Management: Convergence of Credit, Fraud and Compliance. Available here: https://www.experian.com/blogs/global-insights/redefining-risk-management-driving-growth-in-financial-services-through-credit-fraud-and-compliance-convergence/
6. Experian (2025). Experian Global Fraud Report – Key Takeaways. Available here: https://www.experian.com/blogs/global-insights/getting-ahead-of-fast-evolving-fraud-experians-2024-global-identity-fraud-report/
7. Experian (2025). How GenAI is Reshaping Fraud Prevention Strategies experianplc.com. Available at: https://www.experianplc.com/newsroom/press-releases/2025/how-genai-is-reshaping-fraud-prevention-strategies---the-experia.
8. Experian (2025). Proactive Defence: Tackling Evolving Fraud Threats – Available here: https://experianacademy.com/forrester-fraud-research-report-2024/
9. Experian UK (n.d.). Hunter – Fraud Prevention Service experian.co.uk. Available at: https://www.experian.co.uk/business-products/hunter/
10. Experian. (n.d.). Financial crime prevention & compliance. Experian UK. Available at: https://www.experian.co.uk/business/regulation-and-fraud/financial-crime
11. Finans Norge (2024). Norwegian Banks' Fight Against Fraud – Status Report. Available at: https://www.finansnorge.no/siteassets/dokumenter/publikasjoner/svindelbrosjyre-2025---engelsk-versjon.pdf.
12. Forrester Consulting (2024). EMEA & APAC Fraud Survey for Experian. Available here: https://experianacademy.com/forrester-fraud-research-report-2023/
13. VG. (2025, June 17). DNBs toppledere ble utsatt for avansert bedrageriforsøk. VG. Retrieved June 19, 2025, from https://www.vg.no/nyheter/i/jQxk1q/dnbs-toppledere-ble-utsatt-for-avansert-bedrageriforsoek

Reach out to Experian to explore how data, analytics and fraud insights can strengthen your fraud defences today.

Authored by

Jon-Marius Bru
Presales Consultant
Experian Northern Europe

Jakob Færgeman
Global Consultant
Experian Northern Europe