MILKEN INSTITUTE

February 2025

FinTech—What's New and What's Needed

Insights from Asia, the Middle East, and Europe

QUINTUS LIM

About the Milken Institute

The Milken Institute is a nonprofit, nonpartisan think tank focused on accelerating measurable progress on the path to a meaningful life. With a focus on financial, physical, mental, and environmental health, we bring together the best ideas and innovative resourcing to develop blueprints for tackling some of our most critical global issues through the lens of what's pressing now and what's coming next.

About Milken Institute International

Milken Institute International extends the reach and impact of Milken Institute programs, events, and research by focusing on the roles that health, finance, and philanthropy play in addressing social and economic issues around the world. We leverage the Institute's global network to tackle regional challenges and integrate regional perspectives into developing solutions to persistent global challenges.

About the Global Finance & Technology Network

The Global Finance & Technology Network (GFTN) is a not-for-profit organization established by the Monetary Authority of Singapore in 2024 to harness technology and foster innovation for more efficient, resilient, and inclusive financial ecosystems through global partnerships. GFTN organizes convening forums, offers advisory services on innovation ecosystems, provides access to transformative digital platforms, and invests in technology start-ups with the potential for growth and positive social impact through its venture fund.

In partnership with GFTN

GFTN
GLOBAL FINANCE & TECHNOLOGY NETWORK

CONTENTS

Background

In two private roundtables at the 2024 Milken Institute Asia Summit and the 2024 Insights Forum, the Milken Institute and Global Finance & Technology Network gathered leading technologists, development banks, government officials, payment providers, and investors for off-the-record discussions on FinTech. All quotes throughout this report come from roundtable participants. Through these convenings, the Institute hopes to leverage its networks, thought leadership, and experience in innovative finance to help smooth and support the catalytic role of finance and technology in shifting businesses, regulators, and societies toward a more prosperous and inclusive future.

Key Takeaways

- Regulatory initiatives in open finance are expected to increase lending to small and medium-sized enterprises (SMEs), while helping consumers plan their finances long-term.
- Lower transaction fees have enabled the provision of credit lines on real-time payment infrastructures and cross-border remittances through stablecoins.
- Default rates have been surprisingly low among the unbanked, but overly easy access to finance still risks indebtedness, especially when predatory financing is targeted at vulnerable communities.
- AI is increasingly used by both sides: to create malware and intensify social engineering on one hand and, on the other, to power more secure forms of biometric authentication and counter fraud.
- Efforts are ongoing to share fraud data among stakeholders and to make fraud reporting easier. But stakeholders must collaborate to improve the culture of data security across their societies.
- While regulators must be more proactive in innovation and FinTech development, industry players must understand the full range of concerns regarding financial system stability and demonstrate tangible solutions to real-world problems.
- FinTech is just the means to broadening access, uplifting the underserved, and improving societal outcomes. By pursuing these goals with clarity and focus, FinTech innovators can inspire external talents and partners to join their mission.

What's New

The global FinTech ecosystem continues to evolve rapidly, driven by technological advancements, shifting expectations and behaviors, and regulatory changes. When asked "What's new?", participants across the world highlighted several key trends they were observing.

From Open Banking to Open Finance

Participants from Europe highlighted the EU's Financial Data Access (FiDA) framework as a regulatory-led approach to democratizing financial services. FiDA seeks to expand access to financial services data beyond existing open banking initiatives mandated under the revised Payment Services Directive, PSD2. Banks and other financial institutions would be required to share (under consent) the financial data of consumers and SMEs alike with authorized financial institutions and financial information service providers.

But FiDA goes much further than most open banking initiatives. Financial data to be shared encompass not just deposits but also mortgages, investments, crypto assets, pensions, and limited areas of insurance. Data holders must make customer data easily accessible but can also ask for reasonable compensation for sharing data.

Similarly, in Brazil, financial institutions have been sharing foreign exchange, investments, insurance, and pensions data since 2021.[1] Other markets are going even further by requiring data sharing beyond the financial sector ("open data"). For instance, Australia's Consumer Data Right rules cover data sharing between the banking and energy sectors, with more to follow. That said, plans to include the telecommunications sector (telcos) were put on hold in 2023.[2] New Zealand's Customer and Product Data Bill, which covers the banking, electricity, and telcos, is in progress. The UK government released its "Smart Data Roadmap" in April 2024, which will explore data sharing beyond the banking and finance sectors to include energy, retail, transport, homebuying, and telcos.[3]

Experts around the room expected to see increased SME lending as a key benefit of FiDA, drawing on the results of similar initiatives in open banking. In the UK, for instance, the Open Finance Coalition conducted a pilot with HSBC UK that leveraged open finance datasets, as well as data integration and visualization, to provide a more comprehensive picture of SMEs' creditworthiness. Twenty-five percent of SMEs in HSBC's portfolio received a credit offer, while half the SMEs that dropped out of the application process could have received a credit offer had they supplied the additional data required.[4]

Similarly, Bank of England researchers estimated that the Commercial Credit Data Sharing Scheme in the UK increased, by 25 percent, the likelihood of SMEs forming new lending relationships, especially with nonbank lenders.[5] FiDA covers more financial products and countries than the aforementioned examples and is thus expected to have wider-reaching implications.

> *"Having that access to financial services data democratizes the ecosystem for those that are not at the wealthy end of the spectrum. People need assistance in planning for their future, and you've got the long-term benefits that come from open finance."*

As with all ambitious initiatives, however, multiple areas remain unclear. First, the timeline for implementation is short, with provisions kicking in as early as 18 months after FiDA takes effect. Also not yet clear is the extent to which Big Tech would be included or excluded, or how compensation models for data sharing will balance sustainability, fairness, and equity. And unlike Brazil, the EU has not agreed on a uniform format for application programming interfaces.

From Real-Time Payments to Credit

"Ten percent of adults in India have access to credit, while 40 percent get credit from informal sources. But with 350 million users, the UPI can provide a massive distribution channel."

Several participants noted that the provision of credit lines on the Unified Payments Interface (UPI), India's real-time payment system, would be both a step change for the financial system and a massive opportunity for financial institutions. From "mere" real-time payments, scheduled commercial banks were permitted to issue sanctioned credit lines to consumers since September 2023, and smaller banks are now permitted to do likewise.

Participants expected the provision of credit lines to benefit consumers and financial institutions alike. On the supply side, banks can now utilize the massive distribution of the UPI to disburse credit to consumers. On the demand side, the sheer volume of everyday transactions by consumers on real-time payment systems can help financial institutions compute alternative credit scores. Moreover, the continued development of data pipelines and adoption of machine learning will help financial institutions better determine intent to repay.

In addition, participants highlighted the low default rates of the unbanked. Experts from India and the Philippines noted that consumers who lacked access to credit understood that they need to repay their credit lines promptly, thereby earning good credit scores that unlock future borrowing.

"We see a very interesting situation where loans to the lowest end of the market are actually not seeing high defaults because people want to build out their credit score and get it right."

That said, credit provision is a means, not an end, and overly easy access to finance can worsen financial health, especially when predatory financing is targeted at vulnerable communities. "Payday lending" has driven indebtedness in the UK, as have buy-now-pay-later schemes in Indonesia and Malaysia,[6] and microfinance in Cambodia and Sri Lanka.

A participant held regulations responsible for protecting consumers against excess debt. That is not to say, however, that regulations or guidelines will be easy to draft. For instance, when the Singapore FinTech Association put out a code of conduct for buy-now-pay-later schemes in 2022, the Consumers Association of Singapore called for stronger measures the next day.[7]

From Fees to None

"If you're a merchant acquirer, 70 to 80 percent of your costs are tied up in credit card fees. That's not a sign of efficiency, it's a sign of economic rents and an oligopoly. And frankly, that wealth should be redistributed back to society."

In December 2024, the Commonwealth Bank of Australia announced plans to charge customers $3 per staff-assisted cash withdrawal. The subsequent backlash was swift, and the bank put plans on hold the next day.[8] The lessons were clear: Fees are a pain point that decreasing numbers of consumers are willing to tolerate.

Yet, the fact that Bendigo Bank and Adelaide Bank have also imposed fees for staff-assisted withdrawals also points to incumbents' desire to nudge their customers toward more digital forms of banking. As with their customers, banks don't like paying extra costs either.

Drawing a parallel, participants nuanced that the UPI in India was not just a distribution channel. In fact, the UPI incentivizes usage by all parties because, unlike traditional banking, the cost of credit disbursal and recovery is much lower. These lower costs enable financial institutions to supply credit where they traditionally would not.

Other experts noted that these advantages of real-time payment systems were in line with broader trends in the race to zero transaction fees, observing that once-obscure payment innovations were now exploding in user adoption. The clearest example lies in stablecoins, which are increasingly used in developing markets, expanding financial access to the underserved masses. In one 2024 survey of crypto users (not necessarily stablecoins users) in emerging markets, 69 percent of respondents had converted their local currency to stablecoins, 39 percent had purchased goods or services with stablecoins, and 39 percent had sent money to relatives across borders via stablecoins.[9]

"In some regions, people sometimes have just $15 in their bank accounts. Compliance fees for maintaining this account might be $200. But by holding a stablecoin in a digital wallet, individuals can effectively send money anywhere and protect their savings from inflation. And with only $15, the risk of nefarious transactions is very low."

Stablecoins grew in popularity in 2024 due to their reduced transaction costs. The EIP-4844 update to Ethereum in March 2024 slashed transaction fees for the USDC stablecoin on layer 2 networks from US$12 in 2021 to less than US$0.005 on many networks. In comparison, an international wire transfer costs US$44 on average. Indicatively, stablecoin transaction volumes more than doubled that of Visa in Q2 2024.[10]

As the race to zero fees continues, multiple participants believed that Web3 would fundamentally disrupt payments as a fee-generating business model. Even payment providers in the room acknowledged that they had long begun adjusting their business models for the next generation of finance.

From Domestic to Cross-Border

"At least 84 percent of our merchants operate in more than one country, and more than two-thirds of consumers expect to purchase from overseas as part of their normal e-commerce experience."

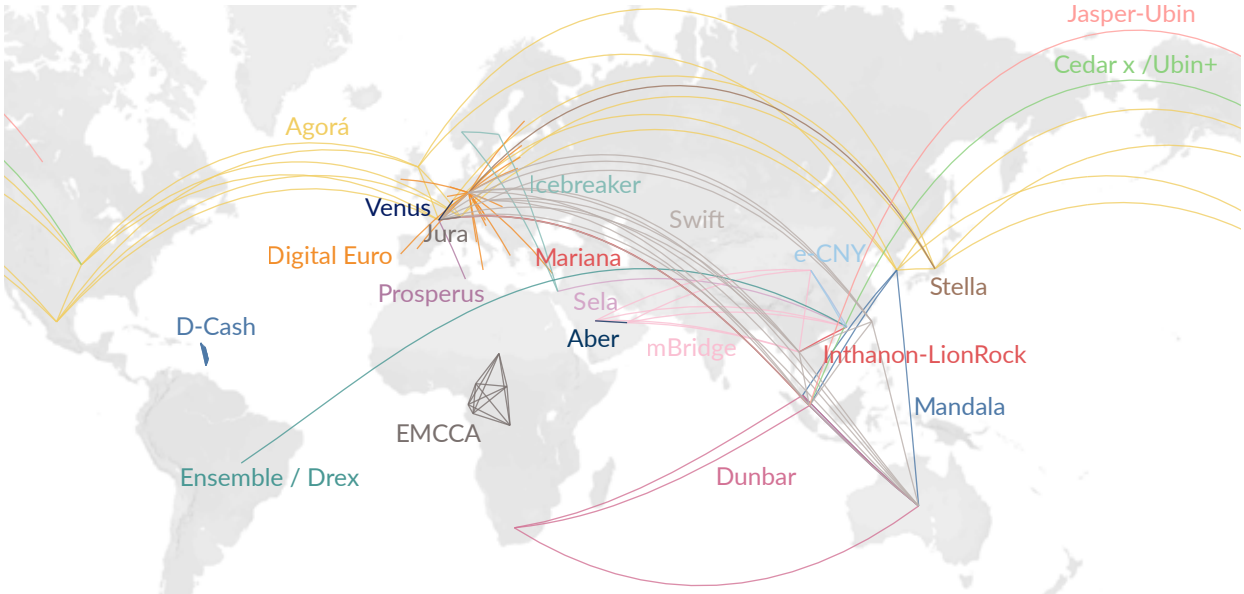
"About 20 percent of the corridor between the US and Mexico is now done through stablecoins, and that's the largest remittance corridor in the world."

The benefits of lower transaction fees can also be felt in cross-border payments. Some participants highlighted that the stablecoins are being adopted faster than the underlying cryptocurrencies themselves because they are slashing remittance costs.

Recognizing the opportunity for impact in remittances, real-time payment systems and, to a lesser extent, central bank digital currencies (Figure 1) are increasingly establishing linkages across borders. Given the volume of remittances, e-commerce, and tourism across the Indo-Pacific, industry participants noted a growing need for payment solutions offering instant status verification, 24/7 processing, and lower costs.

For instance, Singapore has linked its real-time payment systems with Thailand, India, Malaysia, and Indonesia. Georgia is doing so with neighboring Türkiye. Eight out of 10 ASEAN members have signed a Memorandum of Understanding on Cooperation in Regional Payment Connectivity. India has forged relationships with Malaysia, the UAE, and France, while China's WeChat Pay is now connected to Malaysia's PayNet. Tencent is now focusing on establishing linkages with more overseas wallets, allowing tourists to register for WeChat Pay within five minutes.

Figure 1: Cross-Border CBDC Pilots



Source: Milken Institute analysis of various sources (2025)

Participants also noted that bilateral connections, while easier to establish, have poor scalability in more ways than one. First, incentives to connect are weaker where trade or remittance flows are low. Second, bilateral connections are not portable yet grow binomially: 10 countries can have up to 45 bilateral connections, whereas 195 countries can have nearly 20,000 connections, at which point system fragmentation would be debilitating.

On the other hand, multilateral connections allow each country to incur a one-off cost in connecting to the payments systems of other participants present and future. Participants noted the Nexus blueprint by the Bank for International Settlements (BIS) as one example, crediting Singapore for leading its development in Southeast Asia. Project Nexus is now in phase four, where Singapore, the Philippines, Malaysia, Thailand, and India will interconnect their payment systems, while Indonesia has opted to be a special observer.[11]

From Manual to AI

AI is increasingly used to identify and authenticate individuals. One participant raised palm pay as an example of an AI-based, electronic know-your-customer process that allows consumers literally to take payments into their own hands.

Palm-pay technology offers several benefits on top of the security of real-time authentication. To begin with, palm scans identify vein patterns ("vascular biometrics") unique to individuals. This allows palm pay to distinguish identical twins, which facial recognition cannot do. Palm features are also much more difficult to replicate than credit card numbers or facial features. This is not only because palms are harder to misplace than wallets. Vascular biometrics are not visible without scanners and, even if they were, people upload many fewer images of their palms than their faces onto the internet, and far less do they attribute palms to identity. Finally, palm scans are contactless, and thus more hygienic than fingerprinting.

More broadly, secure authentication is becoming increasingly important in the wake of deepfakes. In 2024 for instance, one employee from the design and engineering company, Arup, was tricked into paying out US$25 million to scammers.[12]

That said, while biometric authentication such as palm pay can mitigate identity fraud, it requires even more security and backup measures to be put in place. This is because unlike stolen credit cards, biometric features are very difficult to replace. And unlike credit cards, palm scans require some degree of good health. Hand surgeries, for instance, would likely exclude an individual from palm pay.

Efforts to strengthen biometric authentication, and counter fraud, are ongoing and complementary. On the former, liveness detection (or "proof of human") measures aim to detect if the biometric data presented belong to a person who is real, alive, and physically present. For instance, human skin reflects light differently when compared to photos or screens. Thus, some authenticators check for physical presence by flashing different colored lights during authentication and assessing the reflections.

On the latter, AI can also be used against fraudsters. In 2024, for instance, the British phone company O2 unveiled Daisy, an AI granny meant to waste scammers' time by keeping them on the phone as long as possible.[13] One roundtable participant was also working with a commercial bank in Southeast Asia to intercept deepfakes by using AI.

From Private to Regulatory Innovation

"Finance sector is an ultra-critical sector; we don't want players to just go around trying to find the right approach. Regulatory sandboxes are probably the right way to try out new use cases alongside FinTechs, financial institutions, and market participants to figure out the right regulations in a very controlled, contained way."

"Everyone talks about streamlining physical goods and services, but without the underlying financial technology, it cannot be done properly. We need to ensure Web3 is available to the wider population. This is why regulators are in play from the early stages of experimentation."

Multiple participants highlighted the trend of regulatory innovation. For instance, one participant pointed to how the Saudi Central Bank had come up with multiple regulations from its regulatory sandbox, from buy-now-pay-later through anti-money laundering to embedded payments. Others highlighted how their central banks were experimenting with stablecoins, tokenized assets, cross-border payments, and central bank digital currencies.

For instance, Project Guardian is a collaboration initiated by the Monetary Authority of Singapore and industry players to explore asset tokenization. The World Bank, the International Monetary Fund, and the central banks of France, Germany, Japan, the UK, and Switzerland have also joined the initiative. In parallel, the Hong Kong Monetary Authority set up its Project Ensemble Sandbox in 2024 to experiment with fixed income and investment funds, liquidity management, green and sustainable finance, and trade and supply chain finance.

One participant underscored the rising demand for regulators to be proactive, but stressed that proactivity does not mean revolutionizing the entire financial system in overly ambitious ways that typically make regulators uncomfortable. The participant pointed to the opening remarks at the 2024 BIS Innovation Summit, which highlighted the comple mentarity of small steps (improvements to existing financial infrastructure) and big leaps (fundamental rethinking of financial lives).

What's Needed

For all the advancements in FinTech, much work remains to be done. Participants highlighted the role of regulation in fraud and FinTech development, the need for data collaboration and a culture of data security, and the broader goals of the finance industry and those who might want to work in it.

Fraud Prevention and Mitigation

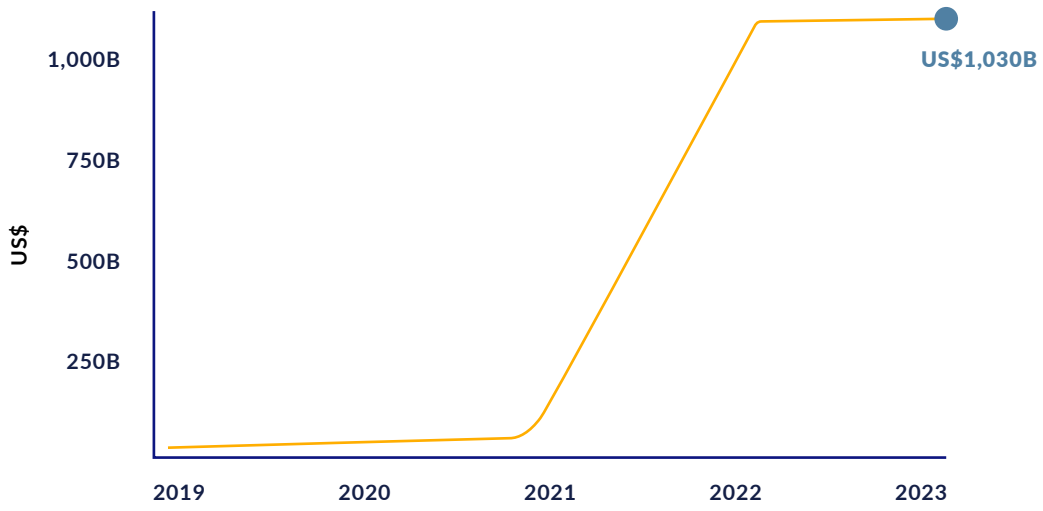
"As we bring people into the financial system, we also increase the risks for newer people who may not understand the infrastructure and ecosystem. So, as we push forward and strive for progress, how do we do so without falling prey to bad actors?"

"You think that FinTech development is very dynamic—but no, the scams landscape is very dynamic. Typologies change all the time, and it's very difficult to remain on top, let alone one step ahead."

Fraud and cybersecurity remained a key concern of participants. In June 2024, Indonesia's Temporary National Data Centre was hit by LockBit 3.0 ransomware, affecting more than 280 public agencies, including immigration services.[14] Ninety-eight percent of the data stored in one of the compromised data centers had not been backed up and, consequently, travelers to Jakarta had their passports processed manually for a fortnight.

Participants warned that recent advancements in AI have made malware more complex and social engineering more credible. Worldwide, the total amount of money lost to scams annually stood at US$42 billion pre-COVID; that figure has ballooned to more than US$1 trillion today (Figure 2).

Figure 2: Funds Stolen by Scammers Worldwide Spiked in Recent Years



Source: Milken Institute analysis of Global Anti-Scam Alliance (2025)

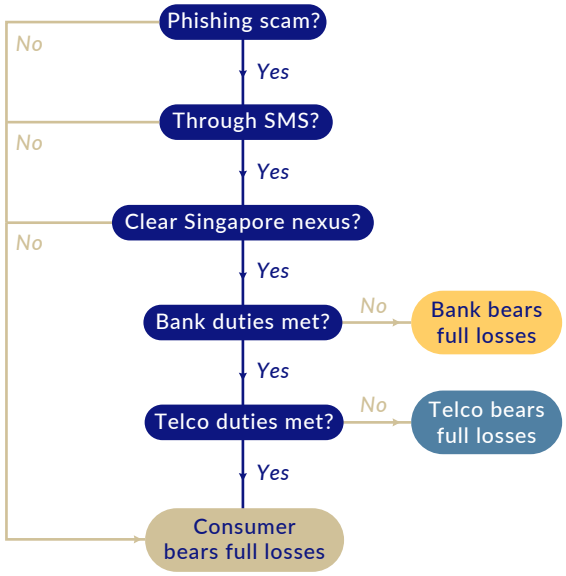
One participant raised the need to support the ecosystem in adopting newer technologies, especially in fraud prevention and cybersecurity. For instance, Fintech Saudi, a government catalyst for FinTechs in Saudi Arabia, implemented a program to provide FinTechs with grants and support for implementing cybersecurity controls in various cloud service providers.

Elsewhere, Singapore has rolled out three key measures in fraud prevention and mitigation. First is money lock, an opt-in feature introduced across major local banks in 2023, that prevents account holders from digitally transferring any of the funds they locked up.

Going one step further, the Protection from Scams Bill was passed in January 2025, allowing the police to restrict the banking transactions of fraud victims who insist on transferring funds to scammers.[15] Restrictions will be imposed as a last resort and last up to half a year, buying time for authorities to convince fraud victims to abandon course. Based on past cases, the police expect to impose five to 10 restrictions a month.

Third is the Shared Responsibility Framework, which took effect in December 2024. The framework specifies the responsibilities required of financial institutions and telcos to protect consumers against phishing (Figure 3). Should any party be found to have breached its duties, it will bear the full losses. Otherwise, the consumer will bear the full losses. The duties required of corporations are very specific and do not cover nondigital communications, emails, WhatsApp, social media, malware, and cases without a clear nexus to Singapore.

Figure 3: Shared Responsibility Framework



Source: Milken Institute analysis of Shared Responsibility Framework (2025)

Regulatory Engagement

Where FinTech has made payment processes much more seamless, it has occasionally and inadvertently led to spillover benefits for fraudsters as well. And, unsurprisingly, participants had divergent views on regulation and trust, and how each related to fraud prevention and the future of FinTech.

"Regulation is actually good; if FinTech has to grow, the regulator has to be stricter and not more lenient."

"I hope we can maintain that focus on consumer advocacy, rather than getting bogged down in overly cautious or politically driven regulation."

"Of course, people want to build big businesses and have a major impact, and we also don't want to be so draconian that we prevent people from doing cool and interesting things. That said, there's definitely an obligation to make sure we're not facilitating abuse."

Such divergence has also been observed elsewhere. In a 2024 survey, FinTechs from the Asia Pacific, EU, US, and Canada listed a favorable regulatory environment as one of the top factors supporting growth, while concurrently citing an unfavorable regulatory environment as one of the top factors hindering growth.[16] As the roundtable discussions progressed, it became clear that rhetorical terms such as trust, regulatory engagement, and the like can at times be unnuanced, one-sided, and even self-serving. This, to some extent, polarizes views among participants.

The view that regulation should not stifle innovation is already well known, as is the need for industry to build trust with regulators, so that the latter are not forced to overregulate in response to crises. But some industry participants had more novel views that payment regulation is ultimately beneficial to the growth and acceptance of FinTech.

One industry expert noted that India's online payments tanked for only a few months after second-factor authentication (2FA) was introduced in 2012 but have since boomed. The Reserve Bank of India is now looking to mandate an additional factor of authentication for most digital transactions.[17] The participant further believed that monetization follows engagement and that FinTechs were vastly outperforming traditional financial institutions in consumer engagement. Hence, as FinTechs grow and continue to eat into the revenue share of traditional financial institutions, they should be able to afford compliance costs.

Another participant remarked that risk-based compliance frameworks should reduce regulatory burdens on smaller FinTechs, and thus would not overburden innovators with compliance costs. Yet another participant warned against scapegoating regulators for what were actually product failures, such as poor consumer adoption of payment innovations.

Obviously, such provocative statements did not go unchallenged, including by regulators themselves. One expert warned that Europe had adopted 2FA long before India but that fraud and cybersecurity are a

cat-and-mouse game that continuously evolves. Europe and Brazil are now having to deal with authorized push-payment fraud, after fraudsters targeted circumventions and exploits to 2FA. In that sense, regulations, however strong, must continuously be tightened, to a point where any company, big or small, would find them stifling.

In addition, the concept of "trust" is frequently discussed in FinTech conversations but often lacks the depth and nuance it warrants. One participant noted that trust between regulators and large institutions can be detrimental to smaller players. Other participants argued that while the concept of risk-based regulations is well known, implementations worldwide from regulatory sandboxes do not go far enough, as evidenced by regulatory arbitrage.

> *"Sometimes regulators become comfortable working with larger institutions that have the resources to engage with regulators. As a result, policies don't always account for the risk profile of different institutions. This forces smaller firms that can't bear the compliance costs to move to lightly regulated jurisdictions. And as the business grows, they may move back to highly regulated regions."*

Yet other participants pointed out how US$274 billion was spent in 2022 complying with anti-money laundering rules, to successfully intercept only 0.1 percent of illicit funds.[18] In some cases, banks have been fined to the point of closure not because financial crime was identified but for failing to tick questionable checkboxes, such as compliance headcounts and budgets.[19] Similarly, a global survey of FinTechs in 2024 saw compliance requirements ranked the third most challenging factor in scaling services.[20]

To be clear, no participant believed that compliance could or should be scrapped. Instead, they expressed hope that privacy-enhancing technologies, and RegTech solutions for fraud detection or sanctions screening, could help mitigate the costs of compliance, better enabling controlled innovation.

> *"As we transition to the Web3 paradigm, it would be amazing if we could take compliance and regulation out of the application layer. In a Web3 context, there's no reason why you couldn't have continuous compliance programmatically embedded in the Layer 1 that you use."*

If participants' polarized views on regulation could be synthesized, they would yield two key strands. First, regulations would be helpful only if regulators were open to learning what they don't know, coupled with broad industry participation in co-drafting policies. On the other hand, while it is admirable that some industry players try to engage regulators early and sincerely, industry may severely underestimate the range of considerations and depth of scrutiny that regulators bring to bear when financial system stability is concerned. It is thus important for innovators to approach regulators as partners and to demonstrate tangible solutions to real-world problems.

"An emerging theme is growing with your regulator. If you want to introduce a payment innovation the local market and regulators have never heard of, it's almost your responsibility to give them a good case study of how and why it would work."

"You can't go to regulators with the attitude of 'We know how to do this, so either you say Yes or No.' What I've found works better is saying, 'How do we do this together? Guide us through this process.'"

"When it comes to emerging technologies, regulators are still grappling with understanding their potential impact on the financial system and broader economy. Innovators must be fully prepared to address very substantive questions regarding monetary policy, financial stability, and the impact of digital assets."

Data Collaboration

"I've been in payments for a long time, and I've noticed that people often view things as either 'the dark side' or 'the light side.' But in reality, it's about finding the win-wins. That's what good payments ecosystems do—they figure out who should partner with whom."

"There is more to be said about the importance of collaboration and sharing because bad actors collaborate and share very well. They might have their own FinTech Festival somewhere out there."

Related to fraud prevention was the need for greater data collaboration: Having collected data on financial fraud, how can financial institutions share them with their regulators and the rest of the ecosystem?

In 2024, for instance, the Monetary Authority of Singapore and six major local banks launched COSMIC, a common data platform for financial institutions to share customer information securely in cases where the customer's behavior exhibits "certain objectively defined indicators of suspicion."[21] In parallel, one participant noted that authorities in China have launched an open data scheme for risk management. Industry players can check against government data for various certifications obtained by merchants, which facilitates merchant onboarding and safeguards consumers.

Saudi Arabia has rolled out similar initiatives under its 2022 Counter-Fraud Framework.[22] One of the responsibilities of counter-fraud departments in financial institutions is the sharing of counter-fraud intelligence—such as emerging fraud typologies or relevant information uncovered by fraud investigations—with the central bank, internal stakeholders, and other external organizations in the sector. For instance, the log-in information of confirmed fraud cases should be shared with the central bank's Sectorial Anti-Fraud Committee.

Saudi regulators have also made it much easier for consumers to report fraud and in greater detail. This is highly important: global surveys have consistently found that the top three reasons victims give for not reporting scams are thinking it would not make a difference, finding reporting too complicated, and not knowing whom to report the scam to.[23]

In agreement, one industry participant warned that smaller FinTechs do not have the capacity to perform fraud detection or share data at the level of payment giants. The participant thus hoped that regulators could employ a mix of enforced and voluntary measures and, at the same time, allow the ecosystem to benefit fully from the scaling of data sharing without making individual participation burdensome.

Cross-border fraud presents an even greater challenge, with more than 40 percent of scams in India traced to other countries.[24] But while financial fraud knows no borders, sharing fraud data between countries runs into the same challenges with cross-border payment interoperability. One participant noted the permanent tension between harmony and autonomy: On one hand, defining global standards requires harmonization of standards worldwide, but on the other, all countries naturally prefer having some autonomy and flexibility in the way global standards are implemented locally. Stakeholders will perpetually need to balance both while attempting to meet their own public policy objectives.

A Culture of Data Security

Also making fraud prevention highly challenging is when societies lack respect for data privacy. For instance, authorities in Hong Kong found that swindlers were harvesting the personal information of job seekers. In 2024, the Office of the Privacy Commissioner for Personal Data investigated the JobsDB platform and eight organizations that had posted anonymous job advertisements.[25] Other participants noted that data could be handled in even more careless ways, stressing that personal data are too easily available online.

> *"Data security is still not taken seriously, and I'm not talking about banks or FinTechs but society … Very often you need to get a photocopy of your social security number. You give it to the photocopy guy, this guy's making two copies, and one copy's being sold somewhere else. Or some NGO collects donors' tax IDs and decides to put that file on their website … The respect for data security, I think there's still a need for it."*

This widespread access to private information makes it unnecessarily easy for scammers to build a comprehensive profile of victims and, in turn, establish credibility with victims, whether by impersonating authorities or family members. Generative AI has also been used to swap faces or clone voices. In turn, the bevy of fraud controls put in place (and paid for) downstream by the financial sector, are undermined.

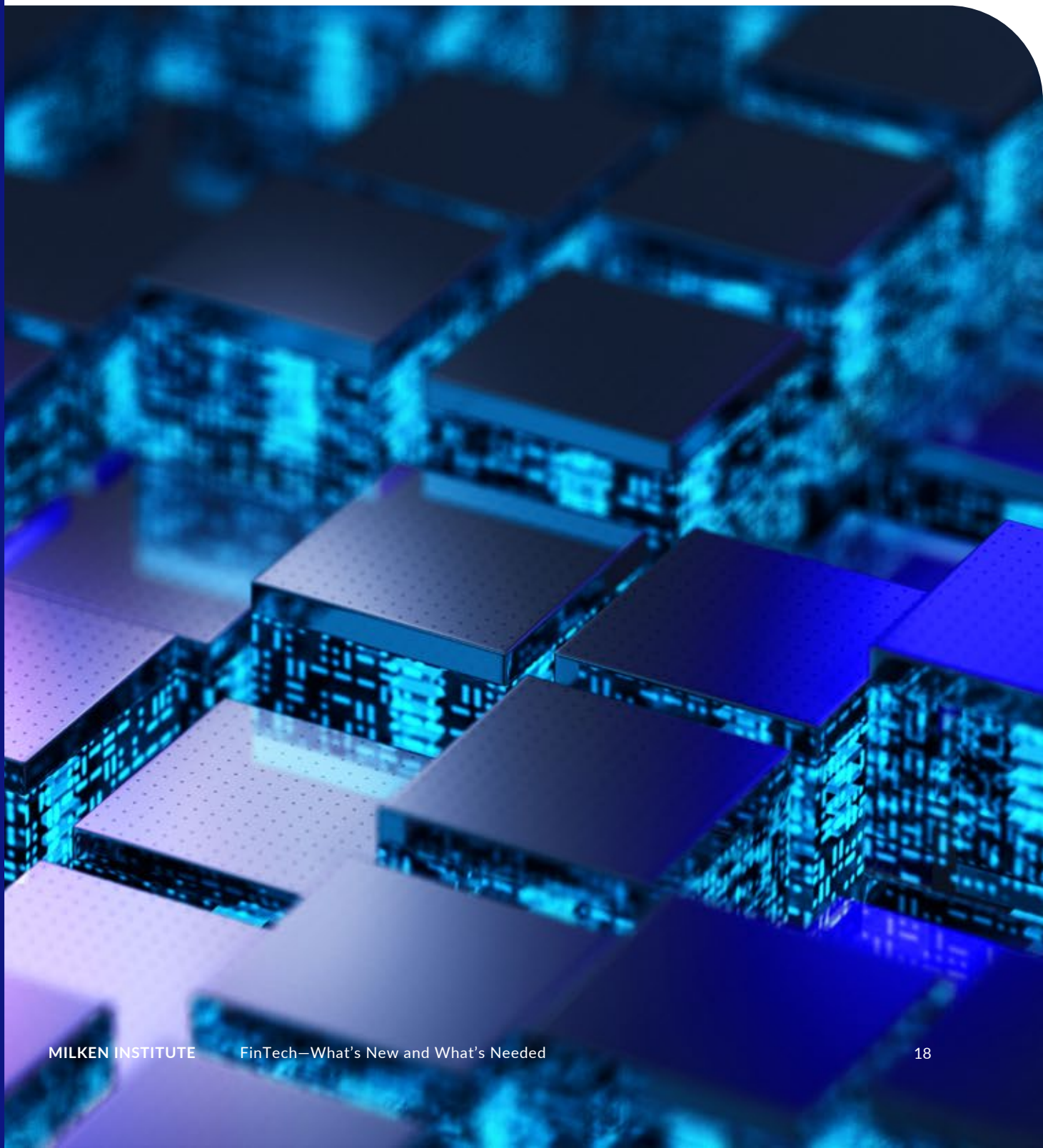
In December 2024, for instance, due to a miscoordination, a Singapore government agency made publicly and freely accessible the unique identification numbers ("NRIC numbers") of individuals in a registry of office holders and business owners, for the purposes of corporate transparency. (Previously, users had to pay nearly US$25 for each individual profile.) While the feature was removed after five days, the damage had been done. Search volumes on the registry more than tripled in those five days, aided by the fact that web scraping defenses were not working as intended. Banks rushed to review their use of NRIC numbers for authentication or as default passwords, while the general public was advised to change all NRIC-inspired passwords immediately.[26]

Blunder aside, this saga partly shows how data privacy is not always straightforward. The Singapore government's underlying assessment was that masking a part of NRIC numbers would give a false sense of security, given that simple algorithms could unmask the remainder. In other words, solutions or policies designed before the digital era could be increasingly outdated and, instead, lull people into a false sense of security.

In other cases, individuals are willing to hand over their personal data but are prevented from doing so. This was most publicly observed amid the pushback of some US-based TikTok users against the US government's banning of TikTok in January 2025. A substantial number of users simply migrated to Chinese apps Xiao Hong Shu and Lemon8 instead, with US-based users on Xiao Hong Shu growing tenfold to 3 million in two days.[27] This partly circumvents any (real or imagined) data protections the US government had intended to safeguard.

Education, awareness, and behavioral change are needed continuously to guard against social engineering, strike balances among security, convenience, and livelihoods, and maintain societal trust in regulations. Most initiatives will entail trade-offs and compromises, in turn requiring broad-based, sustained engagement of and collaborations across all stakeholders to arrive at cohesive outcomes.

"Instead of wanting to own things end to end, it really has to be done with partnerships or we're never going to fulfill the vision of how we aim to create value in the world."



Talent and Purpose

"Today, we're looking for blockchain talents. Where are they gathered? In the tokenized asset or crypto areas, but seldom do we find them in the payment areas."

The final area explored by participants was the need to attract tech talent into the finance industry. The World Economic Forum forecasts that FinTech engineer will be the second-fastest growing job from 2025 to 2030.[28] Yet, participants underscored the difficulty of recruiting technologists who understand the inner workings of finance and vice versa. One expert believed that future opportunities in FinTech lie at the intersection of sectors, and there was a need to encourage both professionals and regulators alike to gain deeper exposure to different sectors—and to do so quickly.

Another participant added that one way to attract talent into finance from other sectors, such as technology, is to focus on purpose and impact: How does FinTech impact and improve the lives of those who need it most? FinTech may have digitized transactions, but it remains to be determined if it has truly broadened access in a way that has uplifted the economic welfare of the underserved and led to meaningful societal outcomes. By pursuing these goals with clarity and focus, FinTech innovators can inspire external talents and partners to join their mission.

"Nobody wants to feel like their finite time and effort are being spent on something that's making things worse rather than better."

"Payments are simpler than people make them out to be. You don't need to be building across 45 different business verticals. At the end of the day, how does this impact the end customer? Focus on solving real-world use cases by finding the right partners and working toward a joint goal."

Endnotes

1. "Open Finance," Banco Central Do Brasil, accessed January 7, 2025, https://www.bcb.gov.br/en/financialstability/open_finance.

2. "Consumer Data Right Rules—Expansion to the Telecommunications Sector and Other Operational Enhancements," The Treasury, Australian Government, accessed January 7, 2025, https://treasury.gov.au/consultation/c2022-315575.

3. "The Smart Data Roadmap: Action the Government Is Taking in 2024 to 2025," Department for Business and Trade, April 18, 2024, https://assets.publishing.service.gov.uk/media/66190f98679e9c8d921dfe44/smart-data-roadmap-action-the-government-is-taking-in-2024-to-2025.pdf.

4. *Embracing the UK's Open Finance Opportunity* (Centre for Finance, Innovation and Technology, February 2024), p.14, https://cfit.org.uk/wp-content/uploads/2024/02/CFIT-Open-Finance-Blueprint.pdf.

5. Tania Babina et al., "Customer Data Access and FinTech Entry: Early Evidence from Open Banking," Bank of England, Staff Working Paper No. 1059, February 2024, https://www.bankofengland.co.uk/-/media/boe/files/working-paper/2024/customer-data-access-and-fintech-entry-early-evidence-from-open-banking.pdf.

6. "US$380 Million and Counting: Rising 'Buy Now, Pay Later' Debt in Indonesia amid Greater Ease of Access," *Channel News Asia*, May 17, 2024, https://www.channelnewsasia.com/asia/buy-now-pay-later-indonesia-consumer-debt-millennials-gen-z-4343856; Rashvinjeet S. Bedi, "'Made Too Easy': Buy Now, Pay Later Schemes Ensnare Consumers in Malaysia in Web of Purchases, Debt," *Channel News Asia*, May 12, 2024, https://www.channelnewsasia.com/asia/malaysia-consumers-buy-now-pay-later-bnpl-credit-personal-finances-debt-4326401.

7. Tang See Kit, "'Buy Now, Pay Later' Code of Conduct Launched to Protect Consumers Against Debt Accumulation," *Channel News Asia*, October 20, 2022, https://www.channelnewsasia.com/singapore/buy-now-pay-later-code-conduct-protect-consumers-debt-3016791; Tang See Kit, " More Safeguards Should Be Included in 'Buy Now, Pay Later' Code of Conduct: CASE," *Channel News Asia*, October 21, 2022, https://www.channelnewsasia.com/singapore/case-more-safeguards-buy-now-pay-later-code-conduct-3019791.

8. Kate Ainsworth, "Commonwealth Bank Pauses Plans to Charge Customers $3 Fee to Withdraw Cash," *ABC News*, December 4, 2024, https://www.abc.net.au/news/2024-12-04/commonwealth-bank-cash-withdrawal-fee-decision-changes/104683232.

9. Nic Carter et al., "Stablecoins: The Emerging Market Story," Castle Island Ventures and Brevan Howard Digital, September 2024, p.16, https://castleisland.vc/wp-content/uploads/2024/09/stablecoins_the_emerging_market_story_091224.pdf.

10. Daren Matsuoka et al., "State of Crypto Repor t 2024," a16z crypto, October 16, 2024, https://a16zcrypto.com/posts/article/state-of-crypto-report-2024.

11. "Project Nexus Completes Comprehensive Blueprint for Connecting Domestic Instant Payment Systems Globally and Prepares for Work Towards Live Implementation," Monetary Authority of Singapore, June 30, 2024, https://www.mas.gov.sg/news/media-releases/2024/project-nexus-completes-comprehensive-blueprint-for-connecting-domestic-ipses-globally.

12. Kathleen Magramo, "British Engineering Giant Arup Revealed as $25 Million Deepfake Scam Victim," *CNN*, May 17, 2024, https://edition.cnn.com/2024/05/16/tech/arup-deepfake-scam-loss-hong-kong-intl-hnk/index.html.

13. Hanna Ziady, "How an AI Granny Is Combating Phone Scams," *CNN*, November 26, 2024, https://edition.cnn.com/2024/11/26/business/daisy-ai-granny-scammers-o2-intl/index.html.

14. Chandra Asmara and Sarah Zheng, "Indonesia's Biggest Cyberattack Prompts Resignation, Audit," *Bloomberg*, July 4, 2024, https://www.bloomberg.com/news/articles/2024-07-04/indonesia-tech-ministry-official-quits-after-june-cyber-attack.

15. Tang See Kit and Ang Hwee Min, "Singapore Passes Law That Gives Police Powers to Freeze Bank Accounts of Scam Victims," *Channel News Asia*, January 7, 2025, https://www.channelnewsasia.com/singapore/scam-prevention-law-restriction-order-bank-account-frozen-4842396.

16. Emina Ajvazoska et al., *The Future of Global FinTech: Towards Resilient and Inclusive Growth* (World Economic Forum and Cambridge Centre for Alternative Finance, January 18, 2024), https://www3.weforum.org/docs/WEF_The_Future_of_Global_Fintech_2024.pdf.

17. Laura Dobberstein, "India Contemplates Compulsory Dynamic 2FA for Digital Payments," *The Register*, August 2, 2024, https://www.theregister.com/2024/08/02/india_contemplates_compulsory_dynamic_2fa/.

18. Elisabeth Krecké, "Why Anti-Money Laundering Policies Are Failing," *GIS*, February 15, 2024, https://www.gisreportsonline.com/r/why-anti-money-laundering-policies-are-failing/.

19. Lanier Saperstein et al., "The Failure of Anti-Money Laundering Regulation: Where Is the Cost-Benefit Analysis?" *Notre Dame Law Review*, Vol. 91(4), December 2015, http://scholarship.law.nd.edu/ndlr_online/vol91/iss1/4.

20. Ajvazoska et al., *The Future of Global FinTech*.

21. "MAS Launches COSMIC Platform to Strengthen the Financial System's Defence Against Money Laundering and Terrorism Financing," Monetary Authority of Singapore, April 1, 2024, https://www.mas.gov.sg/news/media-releases/2024/mas-launches-cosmic-platform.

22. *Counter-Fraud Framework Version 1.0* (Saudi Central Bank, October 2022), https://www.sama.gov.sa/en-US/RulesInstructions/CyberSecurity/Counter_Fraud_Framework.pdf.

23. *Global State of Scams Report 2024* (Global Anti-Scam Alliance, 2024), pg. 22, https://www.gasa.org/_files/ugd/7bdaac_9060be8317424edd9964072cf279a0a4.pdf.

24. Soutik Biswas, "'You Are Under Digital Arrest': Inside a Scam Looting Millions from Indians," *BBC*, November 17, 2024, https://www.bbc.com/news/articles/cdrdyxk4k4ro.

25. "Privacy Breaches Spark Fraud Alert for Jobseekers," *RTHK*, December 9, 2024, https://news.rthk.hk/rthk/en/component/k2/1782705-20241209.htm.

26. "Banks Conducting 'Thorough Review' of Practices on Use of NRIC Numbers: ABS," *Channel News Asia*, December 19, 2024, https://www.channelnewsasia.com/singapore/nric-banks-payment-transfer-security-thorough-review-abs-4816566.

27. Michael Kan, "RedNote's US Users Jump From 300K to 3 Million As TikTok Ban Looms," January 17, 2025, https://www.pcmag.com/news/rednotes-us-users-jump-from-300k-to-3-million-as-tiktok-ban-looms.

28. Till Leopold et al., *The Future of Jobs Report 2025* (World Economic Forum, January 7, 2025), https://www.weforum.org/publications/the-future-of-jobs-report-2025/in-full/.

About the Author

Quintus Lim is an associate director of policy and programs at the Milken Institute. He focuses on policy areas such as R&D financing and technology adoption across domains including health, food, and agriculture, as well as issues of ecosystem building. Lim holds a bachelor's degree in government and economics from the London School of Economics and a master's degree in analytics from the Georgia Institute of Technology.


MILKEN
INSTITUTE