GFTN SELECT - ASEAN SERIES

Philippines: Building the Second Act of Digital Finance.

August 2026

ABOUT

The Global Finance & Technology Network (GFTN) is a Singapore-headquartered organisation that leverages technology and innovation to create more efficient, resilient, and inclusive financial systems through global collaboration. GFTN hosts a worldwide network of forums (including its flagship event, the Singapore FinTech Festival); advises governments and companies on policies and the development of digital ecosystems and innovation within the financial sector; offers digital infrastructure solutions; and plans to invest in financial technology startups through its upcoming venture fund, with a focus on inclusion and sustainability.

GFTN

Innovating Finance. For Everyone.

For more information, visit www.gftn.co

GFTN Select is a series of invitation-only roundtables, held under the Chatham House Rule and designed to facilitate actionable outcomes through meaningful dialogue. It is a platform for shaping policy, technology and financial services roadmaps to guide industry direction, framing greenfield topics with candid discussions amongst key public-private stakeholders to foster innovative solutions and consensus, and driving learning through expert insights and deep, actionable knowledge that empowers informed decision-making. The ASEAN Series brings the programme to the capitals of the Association of Southeast Asian Nations (ASEAN), convening senior leaders around each host market's national priorities. For more information on this edition, visit gftn.co/gftn-select-philippines

GFTN SELECT

Bangko Sentral ng Pilipinas (BSP) is the central bank of the Republic of the Philippines. It is responsible for maintaining price and financial stability, and has led the country's shift to digital payments through its Digital Payments Transformation Roadmap, the national retail payment system and the adoption of digital identity in financial services.

BANGKO SENTRAL NG PILIPINAS

For more information, visit www.bsp.gov.ph

This report is based on the conversations during the GFTN Select – ASEAN Series roundtables held in Manila on 28–29 July 2026, co-hosted by Bangko Sentral ng Pilipinas. All discussions were conducted under the Chatham House Rule to ensure candid dialogue among participants.

CONTENTS

EXECUTIVE SUMMARY

The Philippines is one of Asia's most adaptive fintech markets: a huge and growing remittance corridor driven by overseas Filipino workers, a deeply digital-savvy consumer base, and a sound regulatory architecture for open finance and inclusive payments already in place. The question now is how to scale — how to collectively turn these foundations into credit flowing to micro, small and medium-sized enterprises (MSMEs), real-time payments reaching the unbanked, and AI-driven services that are both powerful and well governed.

It was for this reason that BSP and GFTN jointly convened the GFTN Select Series Philippines on 28–29 July 2026 in Manila: an invitation-only gathering held under the Chatham House Rule, designed for candid, collaborative, peer-to-peer dialogue. It brought together senior leaders from across the financial ecosystem — central bank and securities regulators from the Philippines and the wider region, legislators and government officials, bank and digital bank executives, card networks, insurers, technology firms and development institutions. The timing was deliberate: the Philippines holds the ASEAN chair in 2026, with negotiations on the regional Digital Economy Framework Agreement concluded in Manila in May 2026 and signature due at the summit in November.

The series explored five domains through dedicated roundtables: inclusive instant payments and the commercial models needed to sustain them; AI governance in financial services; agentic commerce and the future of payments; open finance and the pathways to inclusion, competition and trust; and ecosystem resilience across savings, inclusion and consumer protection.

Taken together, the discussions tested how far the existing architecture has carried the market, and where it has not. Participants returned to the commercial models needed to sustain rails priced at or near zero; the accountability that must survive a model an institution cannot inspect; the mandate that voluntary data sharing has so far failed to substitute for; and the distance between a policy on paper and a product in a customer's hands. On the scale question, the constraints identified lay less in technical capability than in economics, accountability and sequencing.

The following pages highlight the key insights from each roundtable discussion.

PART 1:
ROUNDTABLE: INCLUSIVE INSTANT PAYMENTS:
How Do We Scale with Viable Commercial Models?

01
FROM ADOPTION TO OPERATIONAL RESILIENCE

The session opened with a deliberate provocation: if transaction volume were taken away, what would you measure instead? Volume is the headline number every instant payment system reports, and it says little about whether people are genuinely using the system. The answer offered was the share of adults who actually transact, on which participants heard of a rise from 23% to 41% between two survey rounds, the more recent conducted in early 2026. That progress rests on a decade of steady building — a policy framework from 2015, the launch of InstaPay and PESONet for real-time and batch transfers, a move to the ISO 20022 international messaging standard, a national quick-response (QR) code standard, and the addition of bill and government payments, with three further services going live on 29 July 2026. It is also getting cheaper to run: the cost of the central switch that routes these payments has halved as volume has grown.

A note of caution was drawn from a market that reached this point earlier, where success has changed the job rather than completing it: once a system carries enough volume to matter, the work shifts from persuading people to use it towards keeping it safe and available, and supervisory effort in that market has been absorbed largely by fraud and scams. Scale also brings a structural problem. Participants heard of one regional scheme now handling close to 20 billion transactions a year — several times current Philippine volumes — where the rail is owned by the banking industry, so that wallets and other non-banks can reach it only through the very institutions they compete with. That market ultimately had to regulate for open access to resolve it.

"It's not yet time to pop the champagne bottle, but it's still a little win from 23% to 41%."

— Roundtable Discussant

02
ZERO-FEE PRICING AND THE INNOVATION TRADE-OFF

The principle put to the group was that an inclusive instant payment system should be run like a utility: priced to cover what it costs to operate rather than to make a profit, so that the fee a customer pays approaches zero. BSP Circular 1238, issued in June 2026, was credited with pushing person-to-person transfer fees down, with banks already waiving them. The most pointed challenge to that model came from a market where it has been pursued most successfully, and where competition has driven retail prices to zero — and, participants heard, adoption arrived without new products following it. The evidence offered was specific: for several years the authorities in that market have asked its banks to build escrow services, which hold a buyer's money until the goods arrive, for the social commerce platforms where its scam losses concentrate. Nothing has been built.

A different view accepted the affordability goal but questioned the fee implication. Connecting the long tail of billers — utilities, schools, government agencies — to the payment rails means signing up thousands of small organisations one at a time, which is expensive, and the other services sold alongside do not cover that cost, so a service fee is necessary. Since those volumes are growing at double digits, the argument is about recovering investment rather than defending a shrinking business. The opposite case for free pricing was put with equal force: friction rather than technology is what keeps people out, and payments are an entry point to a longer relationship in insurance and later credit, which is where the money is made. One suggestion was that instead of raising fees on digital payments, the true cost of handling cash should be made more visible — framed, when pressed, as a matter of transparency rather than of raising the price of cash.

"They drive the price out to zero. We see adoption, but we don't see new use cases. We don't see new innovation."

— Roundtable Discussant

03

MERCHANT PAYMENTS DEMAND A DIFFERENT DISCIPLINE

Participants noted that instant rails were designed for people paying people, and that paying a merchant is a different discipline. It needs disputes and refunds when goods do not arrive, cashback, reconciliation so that a shop can match payments to sales, and above all merchant qualification — checking who a merchant is before allowing them to accept payments. Without that check, suppressing fraud becomes an endless chase: in a system built so that everyone can hold an account, a fraudster can simply move through thousands of them. This, the discussions emphasised, is the layer instant payment systems were never designed to carry.

The scale of the gap was made concrete with billers. By one operator's account the country has over 1,500 water districts and more than 300 electric utilities, of which only a handful accept real-time payments; connecting the rest means working with each one individually, and paying for it. Another participant set the competitive framing aside altogether, describing a customer's progression rather than a contest between rails: cash first, then instant payments to build confidence in moving money electronically, then access to credit — with credit bureaus, data sharing and the national ID as the layer that makes the last step possible.

"Else you're a whack-a-mole. You're trying to stamp off fraud everywhere you go, because everyone is supposed to have an account. You can run through hundreds and thousands of accounts before you can actually squeeze off the fraud."

— Roundtable Discussant

04

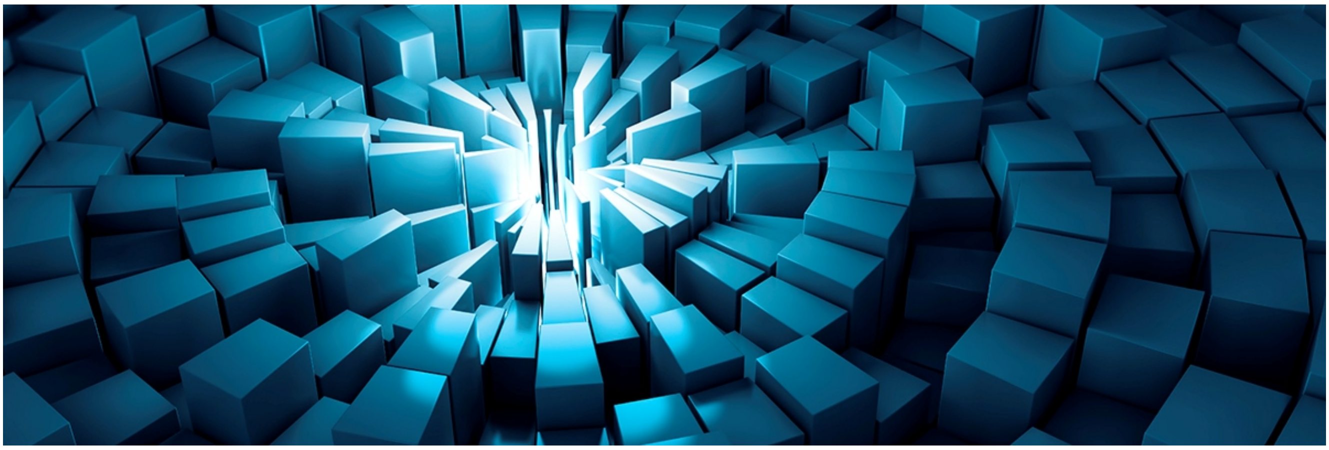
CROSS-BORDER FLOWS AND THE QUESTION OF WHO PAYS

The cross-border discussion moved the question from how fast money travels to what it costs to keep it moving. One provider reported settling about 75% of its payments in under 20 seconds, at a take rate of 51 basis points — roughly half a per cent of the amount sent — and said it had reported moving 12% of all money flowing into the Philippines from abroad in 2024. Its bottlenecks were liquidity and compliance: converting dollars into pesos, ringgit or rupiah at a rate close to the wholesale market requires large volumes, and every market demands its own financial-crime and regulatory staff. The policy ask that followed concerned disclosure rather than price — publishing what a customer actually pays once the exchange-rate margin is counted, not merely the visible fee. On stablecoins the discussion was notably restrained, placing the real opportunity in corporate treasury rather than in consumer payments, and suggesting that even this may fade as conventional rails improve.

Beneath the specifics sat the question the session kept circling. A digital identity system is treated as a public good that nobody expects to pay for. An instant payment system is different in kind: every transaction consumes capacity, and access to it can be withheld — so whether it should be funded the same way is a national choice rather than a settled answer. The final segment, on reaching rural communities and micro-enterprises, produced an observation participants returned to: tuning a system purely to catch fraud inevitably blocks legitimate customers too, and those false alarms fall hardest on rural users with the thinnest digital histories — precisely the people the system exists to reach.

"So the question of who pays is ultimately the question. And these are choices. There's no real right or wrong answer... Digital ID, you don't expect anybody to pay. You see it as a public good. Can instant payment systems be a public good? Even though it is rivalrous and excludable."

— Roundtable Discussant



PART 2:
ROUNDTABLE: AI GOVERNANCE IN FINANCIAL SERVICES:

What Are the Problems Worth Solving?

01
PROPORTIONATE GOVERNANCE FOR TWO KINDS OF AI

One of the key points that emerged, and the one participants returned to most often, was a distinction between two very different kinds of AI in banks. The great majority of what institutions now label AI is work they called digital transformation a few years ago — models that flag suspicious transactions, software that reads documents, automation that moves a case from one queue to the next. It has been running for years, is well understood, and already sits inside existing risk controls. Genuinely new agentic and generative systems, which most institutions do not expect to deploy at scale for some time, carry a different order of risk. The concern raised was that rules written for the second category would land on the first, adding oversight to applications that have worked well while the harder questions went unaddressed.

The group broadly accepted the distinction while cautioning against drawing it too neatly. Governance, another participant responded, is not a single control to be switched on or off; it varies with what the model is used for, and what is right for fraud detection may not be right for credit decisions, cyber defence or personalised marketing. The same participant questioned whether productivity work is safe by definition, offering one example: a simple image-recognition model reading a customer information sheet as a bank moves off paper. If it misreads a figure, the error travels downstream into records and decisions, however mundane the task looks. The conclusion was one of proportionality rather than exemption — governing according to what a system is used for and what happens if it fails, rather than according to the label attached to the technology.

"The spotlight is on agentic AI, or the riskier ones. And yet 95% of what we do are the low-hanging ones... the danger there is you over-regulate the simple ones."

— Roundtable Discussant

02
ACCOUNTABILITY FOR MODELS THE INSTITUTION CANNOT INSPECT

Accountability drew the sharpest engagement of the session. The benchmark cited approvingly was a Singapore requirement that every model have a named accountable person, up to board level. The most constructive proposal made this concrete by analogy with the expected credit loss model — the statistical engine every bank already uses to estimate how much of its loan book will go bad. It is opaque, it is relied on heavily, and it is nonetheless governed by a settled framework covering who builds it, who maintains it, who tests it and how often that testing is done independently. That framework, it was suggested, transfers directly to AI.

The complication raised was ownership. In the previous technology cycle a bank built and held its own models. Now the underlying model usually belongs to one of the same handful of cloud and AI providers everyone uses, and software bought as a service is not obliged to show its workings. The group did not favour moving the burden onto those providers, arguing that regulating vendors would end innovation and that the institution answers for the outcome in any case. One participant then raised the question that went unanswered: if the model is bought as a service, you cannot see inside it, cannot compel the vendor to explain it, and may not understand the explanation if you get one. There was agreement that the institution is accountable, and no account of how it discharges that accountability for a model it cannot inspect.

"To me, the ECL model is a black box, as generative [AI] is. But we rely heavily on it... And there's a whole governance framework on it in terms of who keeps the model safe, who builds it, who tests it, and how often it is independently tested. And I would say that maybe that's the framework that we use for AI."

— Roundtable Discussant

03

A SHARED VOCABULARY BEFORE ANY FRAMEWORK

The most repeated prescription was to set regulation aside for the moment and begin with definitions. Bias, explainability, hallucination and drift — the last meaning a model whose accuracy decays as the world moves away from the data it learned on — mean different things to different institutions; tested independently, participants suggested, the group would produce hundreds of different answers. The argument was grounded in procurement rather than theory. Institutions are buying the same defensive products from the same vendors, and without shared definitions they cannot hold a vendor to a standard, or explain to a regulator why the product they bought was the right one. Absent a common language, a fraud model that wrongly blocks good customers registers as nothing worse than friction.

The task is compounded by foundations that are not yet in place. One participant noted that open finance has not been implemented, that the rules on data security remain unresolved, and that domestic regulations are not harmonised with one another, so that any AI framework would sit on unsettled ground. A related disagreement surfaced over a proposed national register of agentic systems, modelled on the existing requirement to register data protection officers, which would give a court something concrete to test a claim against. Another participant accepted the case for each institution keeping its own inventory of the AI it runs — something a regulator could require immediately — but did not support a national register.

"You cannot govern what you don't understand. You cannot govern what you can't measure. And you cannot govern something that is not standardised across many different layers."

— Roundtable Discussant

04

ENABLING ADOPTION WITHOUT CHILLING IT

A deliberately patient regulatory posture was described. One participant pointed to a strategic sandbox— an arrangement that lets firms test new products live under supervision, with certain requirements relaxed for a defined period — whose participants have begun to move beyond it into wider deployment. Another recalled resisting a premature bill on credit scoring, and expected meaningful rules only once use cases mature. The enabling instinct went further than restraint: relief on the capital banks must hold against AI-related risk for early and safe adopters, and tax relief on the Canadian model for hiring data-science staff, were both floated as alternatives to restriction.

The counterweight was the risk of moving too fast in the other direction. One participant described a credit bureau abroad which, on the day rules making directors personally accountable took effect, cut off all AI access and issued a policy permitting it only in narrow circumstances — the chilling effect Philippine institutions are determined to avoid. Two further threads were highlighted in the discussion. The first concerned employment. Faced with a business-process outsourcing sector employing around 2 million people and earning some US$40bn a year, the government funded AI retraining rather than job protection; the sector closed 2025 with an additional 80,000 jobs. The second concerned infrastructure. On the assessment behind a national AI master plan, the Philippines was said to rank high on policy and regulatory standards, but lagged on computing power. Fewer than a hundred graphics processing units — the specialised chips on which AI models are trained and run — are officially registered in the country, against what was estimated, tentatively, as hundreds of thousands elsewhere.

"We want to avoid the chilling effect. And I think everything is really based on timing."

— Roundtable Discussant

PART 3: ROUNDTABLE:

Agentic Commerce and the Future of Payments

01

FROM TRANSACTION TO MANDATE

It was noted at the outset that the payments system rests on a simple assumption: a human decides, a human authenticates, a human pays. The organising concept the group settled on was the mandate — a standing instruction that software carries out repeatedly on a customer's behalf, rather than simply a faster checkout. Participants pointed to the Agentic Commerce Protocol, an emerging standard for letting software agents transact with merchants, and to card networks issuing tokens, substitute credentials that stand in for a card number, designed to identify an agent rather than a person. The sharpest concern sat at the point of consent. A one-time password or a fingerprint proves that a human is present; neither tells a merchant whose instruction is being carried out when several agents are transacting at once.

On timing, the discussion raised multiple points of view. One view treated the shift as arriving now, citing how quickly digital wallets went from novelty to ubiquity in this market. Another placed it a decade out, on the grounds that it remains unclear who bears the loss when an agent gets it wrong, that merchants may simply decline orders no human placed, and that investment is flowing into AI itself rather than into the payments plumbing around it. The direction was agreed; the sequence was not.

"The business models will change. Payments will change. You will be custodians of trust. And the ones who will come out on top are the ones who have the trust of the consumer."

— Roundtable Discussant

02

FULFILMENT AND DISCOVERABILITY AS THE BINDING CONSTRAINT

Asked which part of the ecosystem is least prepared, the discussion moved well beyond payments, and the most forceful response looked past the payment itself altogether. A transaction is not complete when it is paid for, but when the goods arrive, and the weakness sits in fulfilment — consignments held in traffic, shipments uncleared at the port, stock that is not in the warehouse. A second part of the argument drew particular attention as an inclusion concern. An AI agent choosing where to buy will rank merchants on price, available stock and delivery reliability rather than on branding or advertising, so a small business without the systems to publish that information will not appear in the results at all. Another contribution went further down the stack, arguing that without reliable electricity and upgraded transmission lines - none of it matters.

The discussion was also pulled towards a wider regional prize. The ASEAN Tariff Finder, the region's public tool for looking up tariffs and rules of origin, was held up as the foundation for something larger: connected to real-time payment systems, the trade data behind it could support business-to-business payments well above the low value ceilings that currently apply to instant transfers. The supporting arithmetic on currency spreads and the cost of settlement delay was hedged throughout and does not carry the weight of the argument. What banks want, participants conceded, is not the payment itself but the record it leaves, because a documented supply chain makes lending possible to businesses that are currently invisible to credit assessment.

"The weakness is not in the payments ecosystem. The weakness is in the fulfilment portion, in the merchant portion. The transaction will not be complete if it is not delivered to me, even if it is paid for."

— Roundtable Discussant

03
ACCOUNTABILITY BY DESIGN AND THE LIMITS OF DELEGATION

There was close alignment on one point: the principles of financial regulation do not depend on the technology used, and changing who makes a decision does not change who answers for it. What changes is the demand for accountability by design — recording what was decided at each step, keeping an audit trail, and building in human oversight from the start, rather than assigning blame after something has gone wrong. One participant added the supervisory consequence: the model risk frameworks banks run today were built for a handful of models reviewed one at a time and will not survive the volume that agentic systems generate.

The discussion then highlighted a key issue - hallucination. If the model receiving the instruction cannot be inspected and cannot be relied on to report faithfully, the delegation on which the whole construct rests becomes blurred. A second challenge came from the systemic side. The nearest legal parallels are the rules governing agents and trustees who act on someone else's behalf, but those were not written for a world in which customers write their own automation and model providers may not regard themselves as responsible for what their models do.

"I am going to give mandate to something I cannot really look at in detail."

— Roundtable Discussant

04
THE RAILS DIVIDE BETWEEN CARDS AND INSTANT PAYMENTS

Card schemes already carry the machinery agentic commerce needs — digital authentication, tokenisation and an established process for disputes — so it will land there first. But that is not where Philippine payment volume sits. With credit-card penetration put at around 5% of adults and debit at around 20%, adoption has to happen on the instant rails instead, and it was conceded that the back end is not ready: reconciliation, audit trails, and even returning money credited to the wrong account. Another participant sharpened this into a question of mandate rather than capability. Card networks are not fully inclusive and are not required to be; instant payment systems are national infrastructure with an obligation to reach everyone, including the small merchants cards never will. Yet work on AI standards for those rails has barely started, and the call to accelerate it was the clearest technical ask of the day.

A Philippines-specific observation was offered as to why this may not resolve itself. On one participant's account, no piece of fintech innovation in the market has moved until the largest banks moved — lower transfer fees, electronic identity checks, an early attempt at open banking. And because the industry has moved towards zero transfer fees, a challenger can no longer earn anything from the payment itself and must make its money on deposits instead, which is exactly what it cannot do against entrenched incumbents. Two ways around this were raised: giving an agent direct control of a stablecoin wallet, bypassing banks altogether, and building first for merchants that want to sell to agents before working back to consumers.

"So you're going to have agentic commerce happening on Visa and Mastercard, but not on InstaPay and PESONet, which is really where the adoption will be."

— Roundtable Discussant

PART 4:
ROUNDTABLE:

Open Finance - Alternate Pathways for Inclusion, Competition and Trust

01
A MANDATE AS PRECONDITION, NOT OPTION

The premise for the discussion was that open finance — the arrangement under which a customer can require their bank to share their financial data with another provider they choose — has stalled. The clearest point of alignment was that no market has made it work voluntarily, because large banks rationally treat customer data as a competitive advantage, so an obligation on the largest data holders is a precondition rather than an option. With the technical standards treated as settled, what remains is political will and a clear economic objective.

The legislative answer was also flagged during the discussion. House Bill 9149, the proposed Philippine open finance act, was described as building on the BSP's 2021 framework and adding three things a central bank circular cannot: a binding duty on data holders to share, a statutory right for consumers to own and move their data, and a clear allocation of liability when something goes wrong. Comparative models were then highlighted by the participants. Malaysia mandated a first cohort of the largest banks plus the national provident fund, so that participants receive verified salary history from the outset. Jordan published technical standards first and left the mandate to follow. Vietnam adopted a conditional rule, effective 2027, under which an institution that publishes data interfaces to any outside party — including a related company inside its own group — must publish to everyone. Where the debate still remained was sequencing: wait for the statute, press the regulators to mandate now, or let the private sector move ahead.

"Every market where open finance has been implemented, there must be some kind of mandate for the large data holders. The voluntary model has not worked. There are disincentives for the large banks, and it's very rational — they see the large consumer data set as a competitive advantage."

— Roundtable Discussant

02
VERIFIED INCOME AS THE DECISIVE USE CASE

The discussion highlighted how credit inclusion has stalled on both volume and price, and the root of it is access to verified income: a lender cannot price a loan for someone whose earnings cannot be confirmed. A handful of large incumbents hold what amounts to a monopoly on payroll data, and nothing obliges them to make it portable. The suggestion put forward was two-track — build a mandated central exchange as the long-term destination, while permitting the private sector to move now. The case was reinforced with the observation that tens of millions of Filipinos have been approved for unsecured loans while many more are rejected for want of alternative data, and that scores built from mobile phone usage were reported to separate good borrowers from bad ones more accurately than the credit registry's own files.

Several participants pressed for a perimeter wider than banks, taking in utilities, airline loyalty programmes, retail schemes and statutory contributions. Another participant drew a further distinction between data shared reciprocally between institutions and authoritative records held by the state, which cannot be opened without several regulators acting together. A key observation was that everyone wants to receive data, and that the difficulty begins when it is time to share. Even with the data in hand, whether an institution is willing to lower its credit standards and lend to these customers is a long internal conversation. Mandated access, on that account, may not by itself change lending behaviour.

"The large incumbent players have basically a monopoly on payroll and there's no open finance mechanism to share. And there's no mandated payroll portability."

— Roundtable Discussant

03
TRUST, SCAMS AND THE LIMITS OF SANDBOXES

The discussion opened with a blunt assessment: open finance has stalled while the scammers have moved faster and are several steps ahead of law enforcement and financial regulators alike. One syndicate was described as having taken victims for more than PHP 15bn. The domestic regulatory sandbox — the supervised environment in which firms are meant to test new products before launching — was flagged as having become a freezer rather than a runway, still holding firms admitted two years earlier. The counter-infrastructure was described as embryonic: a fraud identity-sharing network spanning several sectors was launched in 2026, deliberately beginning with negative files only, meaning records of confirmed and suspected fraudsters rather than data on legitimate customers.

Another contribution added a quieter trust problem, which is not whether consumers trust institutions but whether institutions can trust one another's data. Accounts opened legitimately are later sold to others, and nobody is obliged to keep customer records current, so decisions get made on information that is no longer true. Running against all of this, one participant argued the opposite direction of travel: that the bank secrecy law is archaic, should be confronted, and should be accompanied by a public campaign to persuade Filipinos that transparency serves them. Disclosure could thus become an enabler of inclusion rather than the scammer's opportunity.

"While we are building trust for open finance, we must be wary that actually the scammers are many steps ahead of us."

— Roundtable Discussant

04
IMPLEMENTATION AS THE REAL FRONTIER

The Philippines' pilots dominated the practical discussion. A retirement-savings platform was offered as evidence that the machinery works — customer consent, data interfaces, product access — and that technology proved the easiest layer, with governance, operations and the commercial model consuming most of the effort. Comparable wallet-based arrangements elsewhere in the market reach millions of customers, suggesting that scale follows once the product works for the consumer and the incentives work for the distributing institution. A separate contribution located a constraint outside the data question: the product's incentive is a deduction from taxable income, so anyone earning too little to pay income tax gains nothing from it, and a proposal to raise the tax-free threshold would shrink the eligible market further.

The same critique reached the national identity system. A welfare agency ready to open accounts for 2.5 million households found providers unwilling to accept the national ID on its own, asking instead for a stack of additional documents. One response put forward was a simple wallet attached to the national ID that can receive and pay out money without requiring a bank account, which would reach people the current approach cannot, because it serves only those who already have a financial record.

"It's easy to write a law. But how will it be implemented?"

— Roundtable Discussant

PART 5:
ROUNDTABLE: ECOSYSTEM RESILIENCE:
Savings, Inclusion and Consumer Protection

01
INSURING THE INCOME RATHER THAN THE ASSET

The discussion started with a focus on the design of micro-insurance itself. Conventional micro-insurance pays out on death or the loss of an asset, whereas for someone running a small business the real exposure is the income stream, interrupted by serious illness, an accident or a death in the family. Policies should therefore be sized around the number of days of lost earnings a business can absorb before it cannot restart, rather than around a lump sum — and that calculation is possible today, because the point-of-sale systems in small shops record daily takings. Distribution, on this view, must move past the agent selling door to door towards digital partnerships and cooperatives, with cover sold alongside fertiliser and coffee seed, and parametric payouts that trigger automatically on a measured event such as a drought, rather than requiring the customer to file a claim.

One participant questioned the assumption that access is solved, noting that many rural banks are not connected to the instant payment rails at all, so paying a claim in real time fails at the foundation however well the product is built. Another redirected attention from the product to the person: without a path to earning and accumulating something in the first place, there is nothing for an insurance product to attach to. And a further contribution challenged the monetisation premise, noting that resilience rests on health, and that health outcomes can be improved through behaviour change in ways that need not cost the customer anything.

"You're not going for [PHP] 50,000 critical illness cover. You're going for a critical illness cover that pays your loss of income for 14 days."

— Roundtable Discussant

02
LIABILITY FOR THE SMALL SAVER REMAINS UNSETTLED

Trust was framed as the foundation on which every other ambition rests, and scams as the fastest way to lose it. The local threat set was described as fraudulent QR codes, AI-generated bot calls and deepfake scams, alongside the detection tools now offered free to consumers and coordination with the cybercrime and police units. One participant highlighted how the strongest case for sharing data across the industry may not be inclusion at all but fraud prevention, because it is the one use case that spans banks and non-banks together — while personalised marketing and embedded lending, set against already high household debt, are becoming systemically significant across Asia.

Beneath the tools sat the session's structural question. When a small saver loses money to fraud, someone else absorbs it: either the institution that held the account, or the state whose larger purpose is protecting that population. It was agreed that the state must carry a disproportionate share of the compliance cost for the smallest savers.

"One no can erase a hundred yeses. So, you have one incidence of fraud, scam, anything that leads to loss of money that you can't afford to lose, then all of a sudden trust in the system is broken"

— Roundtable Discussant

03

DIGITAL IDENTITY AS A SINGLE SOURCE OF TRUTH

The thread that gathered most force tied three separate problems — the cost of signing up customers, fraud, and consent for open finance — to a single enabler. One participant supplied the economics second-hand, citing banks that spend US$1–US$3 verifying each new customer's identity, a cost that ends up in the price of the product, and a non-bank lender attributing 90% of its fraud to organised syndicates operating across Southeast Asia using deepfaked identities and documents. A national digital identity used as an authentication layer — a service other systems can query to confirm that a person is who they claim to be, as in Singapore and India — would cut that cost, and would also resolve open finance consent by removing the need for every institution to build its own mechanism for proving that a customer agreed.

A clarifying correction followed: what matters for digital finance is not the identity card but the interface through which a bank or wallet can check it. Registration is not the bottleneck — 91 million people were on the national ID at the time of the discussion, and other public services already draw on it. What is missing is a dependable verification service financial institutions can call. A specific execution failure was then flagged: nearly all scams run through a mobile phone, and SIM registration was meant to make phones traceable, but it accepts any of the roughly 75 identity documents in circulation, so a SIM can still be registered under a borrowed or easily forged identity. Requiring the national ID alone would, on that participant's estimate, remove 90% of fraud within a year, and would not need the law amended because only a handful of operators issue SIMs.

"A single authentication layer is not going to be solved bottom-up by industry. It has to be top-down from the public sector, because it becomes a public good."

— Roundtable Discussant

04

MAKING SAVING RATIONAL ON A DAILY WAGE

Participants questioned whether a shortage of financial education is the main issue, suggesting instead that most Filipinos live day to day on low incomes, and that saving sits far down the list of things to spend on rather than beyond understanding. Latent demand was said to be real: tokenised bond issues drew intense interest in higher-yielding products once the minimum investment fell far enough. The paluwagan was offered as a reference point: an informal rotating savings club in which about ten neighbours each contribute a few hundred pesos a week and take the whole pot in turn, without interest — a design template that one digital wallet had considered but never built. Against a National Capital Region minimum wage the speaker put at under US$15 a day, the question raised was what share of that can plausibly be diverted into anything at all.

The contested proposal was a floor under deposit rates, on the grounds that the average rate paid on savings sits far below inflation, so money left in a bank steadily loses value. The counterargument was that better returns come from stronger lending products, a lower cost of doing business and larger banks providing infrastructure to smaller ones, rather than from a mandated rate. Another participant offered a sobering precedent for any subsidy-led answer, recalling an earlier guarantee programme in which the state covered half the risk of lending to small businesses and most banks still declined, while nonetheless proposing a jointly funded resilience facility on the same model. The reframe that closed the session was that the objective is financial health rather than inclusion alone: access and responsible lending must advance together, or inclusion simply produces more over-indebted borrowers.

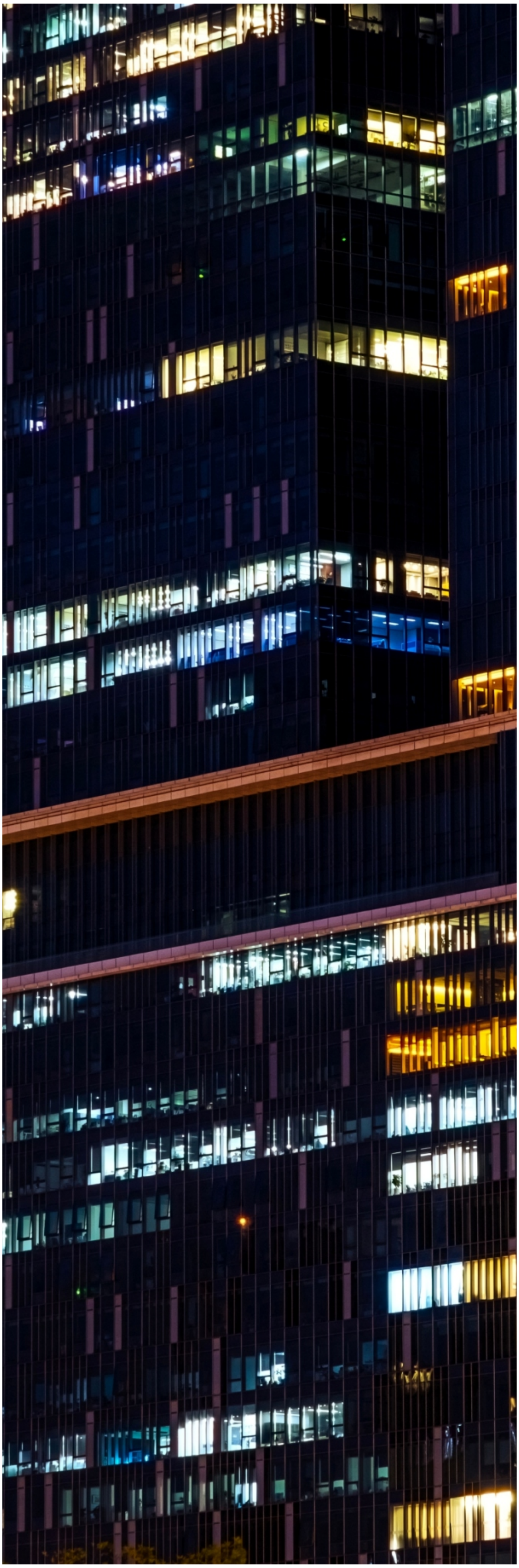
"A lot of things look good on paper... Implementation is a nightmare. And it's a nightmare in the sense not on [the] technology side. It's on incentives alignment."

— Roundtable Discussant

05
LOOKING AHEAD

Held over two days across five roundtables, the discussions spanned instant payments, artificial intelligence, agentic commerce, open finance and consumer protection. Several of the themes raised will shape the next stage of this conversation: how accountability holds when institutions deploy models they cannot fully inspect, whether open finance advances faster through a mandate or through the right incentives, how liability should be shared when a customer loses money to fraud, and how the cost of shared payment infrastructure should be met.

Future convenings in this series will continue the discussion.



GLOBAL FINANCE & TECHNOLOGY NETWORK (GFTN)

6 Battery Road, #28-01, Singapore 049909
gftn.co | hello@gftn.com