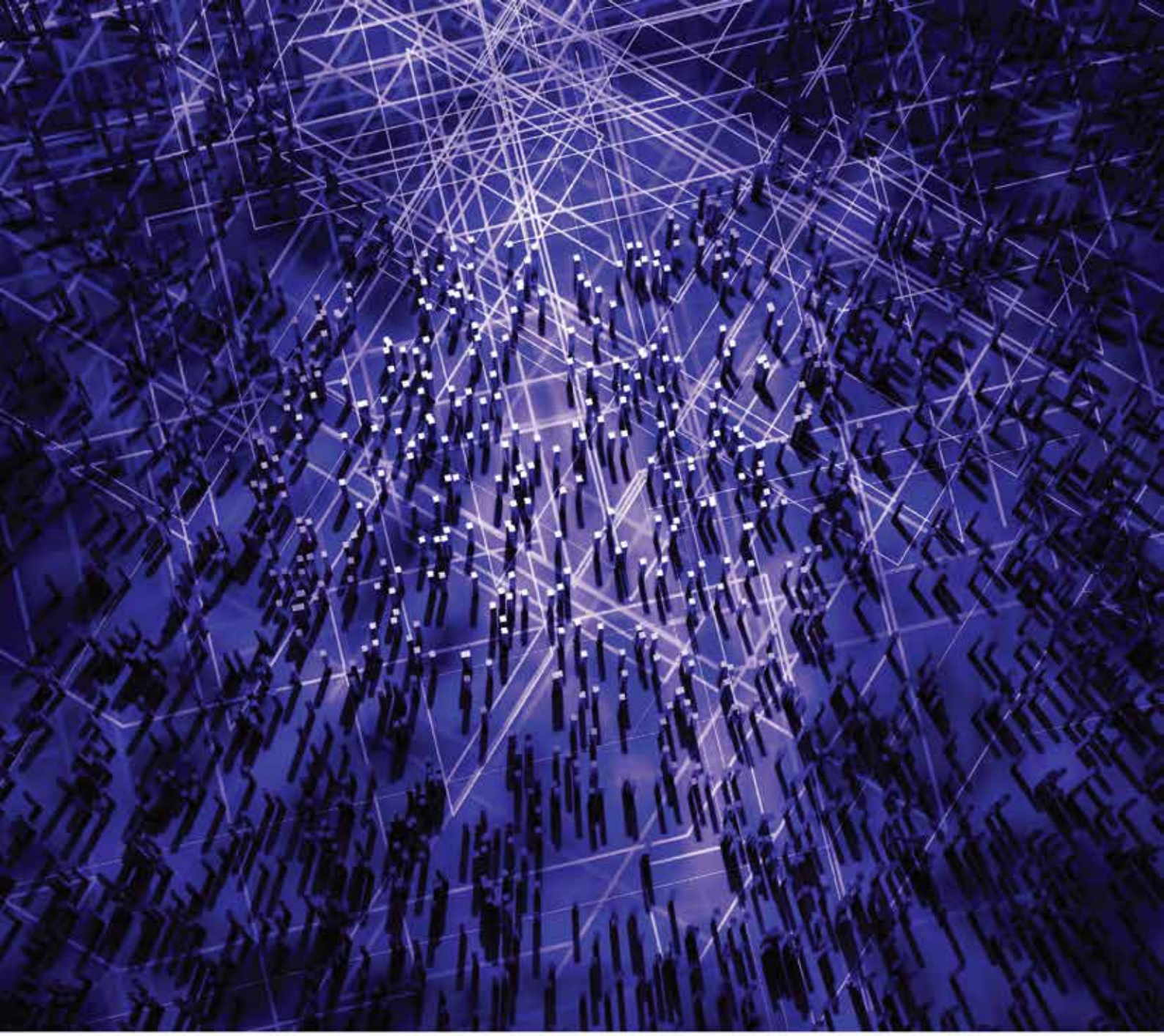
Proof of Human

Building a Human Network for Digital Trust and Scam Resilience in APAC

November 2025

Japan Trust & Safety Association
一般社団法人トラスト＆セーフティ協会

Southeast Asia Public Policy Institute



Proof of Human

Building Human Networks for Digital Trust and Scam Resilience in APAC

November 2025

Japan Trust & Safety Association
一般社団法人トラスト＆セーフティ協会

Southeast Asia
Public Policy Institute

About this paper

This paper has been researched and produced by the Southeast Asia Public Policy Institute in collaboration with the Japan Trust & Safety Association (JTSA) with support from Tools for Humanity to explore the digital trust landscape in the Asia Pacific region. The information and analysis presented are based on interviews with relevant stakeholders, publicly available information, and analysis by the authors. JTSA's strategic contribution—particularly insights from Kiyotaka Tanaka on governance, interoperability, and risk-based PoH implementation—greatly informed the development of this paper.

This paper does not represent the views of Tools for Humanity. It is not intended to be an exhaustive review of policy, legislation, or regulation and should be used with due caution and consideration of its scope and limitations.

Contents

Executive Summary	1
Introduction: The Scam Epidemic and Policy Gap	4
Two Layers of Digital Trust: Digital Identity and Proof of Human	7
Proof of Human: Concept and Policy Relevance	12
Case Studies: Advanced Technology in Practice	18
Conclusion and Recommendations	24
Endnotes	26

Executive Summary

Online scams have become an industrialized, borderless enterprise. The global cybercrime economy now exceeds US$10 trillion, with over US$1 trillion lost to scams annually. Beyond financial losses, scams erode mental well-being, public trust, and drain enforcement resources. The Asia–Pacific region is both heavily targeted and operationally central: Southeast Asia hosts large-scale scam operations, often linked with trafficking, while advanced markets like Japan and Korea face waves of investment and impersonation scams. The problem is regional and interconnected—demanding coordinated responses across economies.

AI voice cloning and deepfakes have industrialized persuasion; automated account creation enables mass reach; and crypto and instant payments accelerate monetization. Yet the same technologies can also strengthen trust through better identity assurance, authenticity signals, and privacy-preserving safeguards—supported by governance and transparency to prevent new risks.

Existing enforcement and awareness efforts are necessary but insufficient when criminals can cheaply create thousands of synthetic or automated identities. Sustainable progress requires two layers of digital trust that close the gaps scammers exploit:

- **Digital Identity (Digital ID):** Answers *"Who are you?"*—non-anonymous, KYC-capable credentials for regulated contexts (finance, e-gov).
- **Proof of Human (PoH):** Answers *"Are you a real, unique human?"*—privacy-preserving signals usable in open, cross-platform environments where full identity disclosure is neither needed nor desirable.

PoH is not a substitute for Digital ID. It is a complementary layer that extends trust to the parts of the internet where most scams originate (social, messaging, marketplaces), reducing fake/synthetic accounts and bot-driven abuse while preserving user privacy. Recent developments underscore the need to deploy PoH within a trust and safety-based framework—ensuring it addresses automation and scaled abuse without being misinterpreted as a guarantee of user intent or trustworthiness.

Across APAC, governments have built strong digital ID foundations that strengthen KYC and accountability in regulated sectors, but most scam activity originates in unregulated spaces such as social media, messaging, and online marketplaces, where Digital ID does not apply. This is where PoH adds unique value: through mechanisms such as privacy-preserving human tokens and device-based verification, PoH can limit mass fake account creation, disrupt bot-driven fraud operations, and strengthen authentic human networks before victims are targeted. To succeed, these technologies require clear safeguards, user control, and governance structures that prevent misuse, protect anonymity, and maintain public trust.

Case Snapshots

Japan — My Number: State-verified uniqueness at scale but trust challenged by data-handling incidents; a candidate anchor for hybrid models pairing government ID with PoH for privacy-preserving verification beyond government services.

South Korea — Real-name regime: Deep integration across finance, telco, and e-gov effectively acts as a PoH proxy; success tempered by privacy/civil-liberty concerns—driving interest in user-controlled, decentralized authentication.

Malaysia — MyDigital ID (rollout): Biometric-linked credentials tied to the national registry; governance-by-design trajectory aligns well with PoH principles but requires strong safeguards and public trust to scale.

Philippines — PhilSys (rapid scale): Fast, mass adoption with digital ID download and e-verification; demonstrates operational PoH-like functionality, alongside the need to keep governance and user education apace.

Effective scam resilience requires layered assurance: regulated interactions bound to verified identities, and open platforms fortified by privacy-preserving proof of humanness. Transparency, interoperability, and user control are the cross-cutting enablers. Neutral governance mechanisms—whether standards bodies, industry intermediaries, or multi-stakeholder frameworks—will be critical for translating national requirements into operational practices for global platforms.

Policy Recommendations

Integrate Digital ID and PoH into scam-prevention strategies: Embed proof-of-uniqueness checks in financial, e-commerce, and communications flows to curb impersonation, synthetic identities, and bot abuse, guided by trust and safety-based deployment and safeguards that prevent overreliance.

Support privacy-preserving, interoperable standards: Pair biometric/credential assurance with cryptographic techniques (e.g., zero-knowledge proofs) to protect anonymity where appropriate and enable cross-border usability, while ensuring PoH cannot be repurposed for tracking or profiling.

Promote regional policy dialogue and coordination: Use platforms like the APEC Business Advisory Council, G20 High-Level Principles for Digital Financial Inclusion, and UN digital-economy initiatives to align objectives, share evidence, and pilot PoH-enabled verification across sectors, including sandbox testing to assess usability, inclusion, and proportionality."

Scams expose a structural trust deficit. A combined Digital ID and Proof of Human architecture—implemented with strong privacy, governance, and interoperability—can raise the cost of abuse at scale while preserving user rights, accelerating Asia's path to a safer, more inclusive digital economy.

Introduction: The Scam Epidemic and Policy Gap

As societies and economies have embraced digital technology, online crime has surged in scale and sophistication. The global cybercrime economy is now worth over US$10 trillion, positioning it as equivalent to the world's third-largest economy by GDP.[1] Scams are a specific and growing type of cybercrime with consumers losing more than US$1 trillion annually to scams.[2] However, the costs extend well beyond balance sheets: victims experience lasting harm to mental health and wellbeing, confidence in digital services and the digital economy erodes, and public resources are diverted to enforcement, awareness, and national cybersecurity efforts.[3]

Asia's Dual Role

Among this global epidemic of scams, the Asia Pacific region stands out as the most heavily impacted. So-called 'pig-butchering', investment or romance scams, where scammers use social engineering techniques to build relationships with victims and deceive them into making payments or investments, are especially widespread. These are often initiated through social media or messaging services, by large-scale scam operations in dedicated scam centers operated by transnational organized crime syndicates.

Southeast Asia sits at the center of this economy: as a source of scam victims, as a hub for operations in unregulated regions, and as a source of workers, many of whom are also victims of human trafficking.[4,5]

Meanwhile, advanced markets in the APAC region such as Taiwan, Japan and South Korea are closely tied to this dynamic: they are high-trust, digitally mature economies whose consumers are frequent targets of investment and impersonation scams, and they have also seen their own nationals lured into overseas scam centers.[6] Together, these dynamics underscore how the region's crisis is not only local but part of an interconnected Asia-wide challenge, demanding coordinated responses that bridge both advanced economies and trafficking-affected states.[7]

Technology: both an enabler and a solution

Technology has fundamentally altered the economics of scamming, and even the best-resourced governments struggle to keep pace with the rapid evolution of methods.

First, persuasion has been industrialized. Artificial intelligence, voice cloning, and deepfakes are being weaponized to facilitate fraud, with over 42 percent of financial-sector scam attempts attributed to AI.[8] These tools can deliver hyper-realistic scripts, images, and calls in multiple languages, enabling long-con "investment" or romance schemes to be run by relatively unskilled operators following playbooks refined through A/B testing.

Second, scaling has become effectively limitless: automated account creation, SIM farms, and cross-platform tooling allow small teams to contact millions across social media, messaging, and telephony within hours, while bots and recommendation systems can be gamed to identify receptive audiences.[9]

Third, criminal innovations in monetization have accelerated. Cryptocurrency infrastructure, fintech channels, money-mule networks, and cross-chain mixers enable rapid movement and obfuscation of funds, while instant payments and fragmented KYC/KYB regimes reduce the window for interdiction in traditional banking.[10]

The result is a structural trust deficit in the digital economy: criminals are adopting and adapting new tools faster than governments and regulators can respond.

The same technologies that enable abuse can, if deployed at scale with safeguards, restore confidence.

Stronger digital identity and entity assurance—privacy-preserving verification of people, devices, and businesses; SIM/number reputation; and higher-assurance options for high-risk flows—can raise the cost of mass targeting.

Authenticity signals for content and communications—such as cryptographic provenance for images and video, verified caller/sender frameworks for voice and messaging, and hardened ad and account-integrity controls—can reduce successful impersonation.

Privacy-preserving signal-sharing across platforms and payment networks can help detect coordinated abuse, while real-time payment risk-scoring and "cool-off" frictions (confirmation of payee, stepped-up checks, delayed settlement for suspect transfers) can cut losses at the point of execution.

A victim-centered model—rapid takedown routes, faster fund-recovery rails, and clear pathways to identify coerced workers as victims—must complement enforcement to break the cycle of exploitation.[11]

Technology is therefore both an enabler of criminal activity and a necessary part of the solution. Governments, platforms, and financial institutions must continually adopt and update defensive technologies at the same pace that criminals innovate, because scams are not simply cybercrime incidents, but symptoms of a deeper structural trust deficit in the digital economy.[12]

If scams reveal the fragility of online trust, then reliable digital identity (ID) is one of the clearest tools available to repair it. By providing verifiable assurance of who is behind a transaction or interaction, digital ID raises the costs of abuse while supporting safer digital economies. The next section explores the problem digital ID is designed to solve, the technologies involved, and emerging policy responses in the region.

Two Layers of Digital Trust: Digital Identity and Proof of Human

Combating scams requires layered systems of trust. Enforcement and awareness are vital, but sustainable progress depends on identity and authenticity mechanisms that close the loopholes criminals exploit at scale. Digital Identity (Digital ID) and Proof of Human (PoH) represent two complementary, yet fundamentally different, layers of this trust infrastructure. Digital ID answers "Who are you?" by linking individuals to verified, real-world identities recognized by banks and governments, while Proof of Human answers "Are you human?" by confirming humanness and uniqueness without revealing identity. One is non-anonymous and suited for regulated environments such as banking and e-government; the other is anonymous but verifiable, securing open digital spaces where full identity disclosure is neither required nor desirable. Together, they create a balanced foundation that supports both accountability and privacy in digital economies.

Proof of Human is not a substitute for national digital ID systems; it is a complementary, privacy-preserving layer that extends trust to parts of the digital environment where full identity verification is neither feasible nor desirable.

Forms of digital ID technologies

Digital ID solutions exist in multiple forms, each addressing different risks:

Credential-based digital identity systems rely on digitally issued and verifiable credentials, often derived from government-issued ID or trusted institutions such as banks, mobile operators, or universities, to securely assert identity attributes such as name, age, or nationality. These credentials can be stored in a digital wallet and presented across services, enabling reusable, privacy-preserving digital interactions that are far more robust than simply linking scanned documents to login credentials.[13]

Biometric authentication verifies that the person accessing a service matches the individual previously enrolled, using unique physical or behavioral traits such as fingerprints or facial features. This helps prevent unauthorized access, even when other credentials like passwords or devices are compromised. Importantly, biometrics authenticate the user but do not in themselves confirm identity.[14]

Hybrid digital identity models combine multiple factors, such as government-issued credentials and biometric authentication, to create a reusable, high-assurance digital identity. These systems are designed to support cross-platform interoperability, strong authentication, and privacy controls.[15]

All are KYC-enabled and non-anonymous by design, as they are intended for traceability, compliance, and accountability within regulated ecosystems.

Policy Responses in APAC

Digital ID technologies cannot succeed in isolation; they require supporting policy frameworks that set standards, ensure privacy, and promote broad uptake. In practice this means:

- Clear regulatory recognition, so that digital ID carries legal weight in financial transactions, contracts, and public services.
- Robust safeguards to protect personal data, with requirements for secure storage, limited use, and redress mechanisms in case of misuse.
- Public-private and cross-sector adoption, ensuring that IDs are recognized not only by governments but also by platforms, banks, and utilities that are often at the front line of scams.

Across Southeast Asia, governments are steadily advancing digital ID systems as foundations for more trusted digital economies.

Thailand's National Digital ID (NDID) platform links banks, telecom operators, and state agencies in a federated framework.[16]

Indonesia and the Philippines are rolling out national e-ID programs tied to financial inclusion and social services.

Vietnam has begun embedding biometric verification into its e-government portals.

While the level of maturity varies, the regional policy momentum is shifting from building national systems to exploring interoperability. Policymakers increasingly recognize that mobility, migration, and trade flows demand IDs that can be recognized across borders, not just domestically.

In more advanced economies, comprehensive national ID frameworks are already in place and moving toward deeper integration.

Singapore's SingPass anchors access to banking, healthcare, and e-commerce.[17]

South Korea is expanding its national resident registration system into a fully digital identity platform that integrates e-government services, financial transactions, and mobile authentication.

Japan's "My Number" system provides every resident with a unique 12-digit identifier, which is increasingly linked to healthcare, taxation, and administrative services.[18] Efforts are also underway to extend its utility into financial services and cross-border recognition.

These trajectories differ in scope and speed, but together they illustrate how national-scale credentialing can evolve beyond secure logins to become the institutional backbone of digital economies, while offering reference points for ASEAN governments models considering domestic implementation or regional interoperability.

At the same time, these experiences highlight that government action alone is not enough. The effectiveness of Digital ID ultimately depends on its integration across the wider digital ecosystem through cooperation between governments, financial institutions, and technology platforms.

The Role of Digital Identity in Combating Scams

Digital ID technologies are among the most promising systemic tools to counter scams and fraud. By authenticating people, devices, and organizations in a verifiable, non-anonymous manner, Digital ID systems reduce impersonation, limit anonymity, and raise the costs of abuse. While not a silver bullet, they form the KYC-capable backbone of digital trust, ensuring that regulated transactions and services are tied to real, accountable individuals or entities.

Closing the gaps that scammers exploit

Scams thrive on gaps in verification. Fraudsters use bots and fake accounts to spread messages at negligible cost, deploy deepfakes and voice clones to impersonate trusted individuals, and hijack legitimate accounts to defraud victims. Weak or inconsistent authentication across platforms means these attacks succeed far more often than they should.

Digital ID closes this gap on the regulated side: by binding digital interactions to verified identities, it becomes harder for criminals to operate anonymously and easier for victims, businesses, and regulators to trust who they are dealing with online. However, most scams originate in unregulated spaces, such as social media, messaging apps, and informal marketplaces, where KYC systems do not apply. Addressing those environments requires a different, privacy-preserving approach such as Proof of Human.

Yet even the strongest Digital ID system cannot fully address scams driven by fake accounts and automated abuse. This gap has prompted growing interest in emerging concepts such as Proof of Human, which explore privacy-preserving ways to verify that a user is real without requiring personal identification.

Proof of Human: Concept and Policy Relevance

Definition of 'proof of human'

Proof of Human (PoH) represents a new novel and evolving approach to strengthening digital trust. It is commonly defined as a system designed to prevent multiple fake identities, providing verifiable assurance that an online actor is a real human being rather than an automated bot or fabricated identity.[19] Unlike simple account sign-ups or CAPTCHA challenges, PoH aims to provide a persistent, reusable signal of humanness that can be recognized across platforms and services without disclosing more personal data than is necessary—laying the foundation for more trustworthy human networks across the digital ecosystem.

Importantly, PoH does not replace or compete with national digital ID systems. Instead, it complements them by addressing a different layer of the trust problem, verifying that a user is human rather than establishing who that user is.

Conceptually, PoH differs from other layers of digital assurance. Traditional digital ID frameworks answer the question "who are you?" by linking individuals to verified attributes such as names or national registration numbers. Authentication tools like passwords or multi-factor codes protect accounts once created, but they do not prevent the creation of fake or synthetic profiles in the first place. For nearly two decades, CAPTCHAs tried to fill that gap by testing whether users could solve puzzles as a proxy for humanness. Yet their effectiveness has declined as bots and AI tools increasingly outperform humans, while also creating friction for legitimate users. PoH, by contrast, addresses the prior question "are you human?", a form of assurance that aligns with broader efforts in verified credentials, bot mitigation, and what blockchain communities call sybil resistance. In this sense, PoH is part of a wider lineage of innovations aimed at balancing authenticity, privacy, and scalability in digital ecosystems.

Forms of PoH Verification

Proof of Human systems can be implemented in several ways, each offering different levels of assurance and privacy. The table below outlines the main forms of PoH verification and how they work in practice.

Type of PoH Verification	How it works	What the user experiences	Example Use Cases
Biometric-based (privcy-preserving)	One-time liveness check (e.g., blink/turn head). System issues a cryptographic “hu-man token” without storing or sharing bi-ometrics.	A short, one-time ver-ification similar to unlocking a phone; no identity data dis-closed.	Prevents mass fake accounts; high-assurance PoH for platforms handling financial or high-risk transactions.
Device-/ hardware-based	Device attestation confirms a real, non-emulated device; can bind “one human = one device” without knowing identity.	A background check embedded in the sign-up process, no biometrics required.	Limits bot farms; re-duces automated ac-count creation in messaging apps, so-cial media, or gaming platforms.
Interaction-/ challenge-based	Users complete liveness-like prompts or cryptographic chal-lenge–response tasks that bots cannot reli-ably perform. No bi-ometric data used.	Simple human-interaction tasks (e.g., controlled motion, timed prompts), but far less intrusive than traditional CAP-TCHAs.	Useful for social plat-forms and online communities to deter synthetic profiles without requiring ID or biometrics.
Social / web-of-trust attestation	Users are verified by trusted community members or reputation networks; plat-form converts this into a PoH signal.	A lightweight en-dorsement or confirmation from verified users/communities.	Peer-to-peer market-places, gig platforms, or community-based verification environ-ments.

Table 3.1: Forms of Proof of Human (PoH) Verification

How ‘proof of human’ can help fight scams

While still a novel concept, PoH has potential relevance in the fight against scams and fraud. Online fraud today is powered by scale: traffickers and criminal groups create thousands of fake accounts to lure victims, automate pig-butchering scams, or operate networks of money-mule accounts. The ability to manufacture digital personas cheaply and in bulk lowers the cost of fraud while overwhelming the capacity of platforms and regulators to detect malicious activity. PoH, by contrast, can help shift the balance by strengthening authentic human networks, limiting the spread of synthetic or automated identities at scale.

In principle, PoH could introduce friction at the point of account creation or transaction, limiting the speed and scale of fake account proliferation.

Verifiable humanness can serve several functions:

1. Prevent fake profiles that act as bait in romance, employment, or investment scams. Instead of relying on reactive takedowns once victims have already been drawn in, PoH can help reduce the supply of fraudulent accounts from the outset.

2. Protect financial systems by reducing the flow of transactions through mule accounts. Banks and payment networks often struggle to distinguish between legitimate users and fraudulent accounts; a reusable signal of humanness could strengthen existing KYC and AML safeguards without requiring constant disclosure of personal data.

3. Reinforce trust in digital commerce and online communities. In markets where scams and impersonation have eroded confidence, being able to verify that a buyer, seller, or community member is a real person may eventually help restore confidence in peer-to-peer exchanges, gig work platforms, and social spaces.

Safeguards and Governance

Safeguards are essential to ensure that PoH does not itself become a tool of surveillance. Emerging models emphasize *privacy-preserving design*. Cryptographic proofs and zero-knowledge methods enable users to demonstrate humanness without exposing underlying identity data. This distinction between identity verification (is the actor human?) and *identity disclosure* (who is the actor?) is critical for maintaining rights and trust across jurisdictions. Safeguards also require strong governance: oversight by regulators, standards bodies, or multi-stakeholder audits can help prevent PoH signals from being repurposed for intrusive tracking or profiling.

Equally important are user rights and inclusion. Verification should be voluntary, transparent, and revocable, with individuals able to understand and control how their PoH signal is used. Complementary tools such as age-assurance mechanisms can protect minors without requiring disclosure of sensitive information, while multiple pathways to verification help avoid excluding people without smartphones, biometrics, or stable connectivity. The credibility of PoH will ultimately depend on whether it can improve security while respecting privacy, ensuring accessibility, and aligning with regional commitments to digital trust.

Yet technical safeguards alone are not enough. Effective PoH deployment requires governance structures that reflect the realities of digital ecosystems in APAC. National digital ID systems operate under domestic rules, while most real user interactions—and most privacy-sensitive risks—occur on global platforms. Because of this structural gap, direct integration between governments and platforms is rarely feasible on its own. A neutral governance layer is often needed: independent interoperability intermediaries that can translate requirements, convene stakeholders, and support safe testing before large-scale adoption.

Such intermediaries can help ensure that PoH is implemented in ways that are technically realistic, privacy-respecting, and aligned with both national frameworks and cross-platform environments. They can translate domestic standards into operational guidance, host multi-stakeholder discussions on privacy and auditability, and facilitate sandbox environments that allow PoH to be trialed safely without unintended risks to users or platforms.

A further safeguard relates to public trust. PoH is a new concept—distinct from digital identity, authentication, or eKYC—and misunderstanding can easily create concerns about surveillance or data use. This is why capacity-building is just as important as the technology itself. Neutral intermediaries, industry groups, and civil-society networks can help explain how privacy-preserving designs work, reinforce that PoH answers “Are you human?” without revealing “Who are you?”, and offer practical guidance for responsible implementation. Strong communication and user education are ultimately what translate a well-designed PoH system into something people feel comfortable adopting.

Finally, PoH must be embedded within a trust and safety framework. Verifying that a user is human does not guarantee that the user’s intentions are safe. Many of the most harmful scams in APAC—such as investment fraud, impersonation scams, and long-form social-engineering schemes—are perpetrated by real human operators. This is why PoH should complement, rather than substitute, other safety signals. Applying frameworks such as ISO/IEC 25389 (the Safe Framework) helps ensure that PoH is used appropriately:

- as a layered defense against automation and scale attacks;
- alongside behavioral and reputational signals that detect human-driven threats;
- with clear implementation guidance to avoid overreliance.

PoH should therefore be piloted as a complementary innovation, not a substitute, to reinforce existing identity frameworks. If designed and governed carefully, it could help test new ways of verifying real users in high-risk digital environments, contributing evidence for what might work at larger scale. More broadly, interoperable and rights-respecting PoH frameworks could complement national digital ID initiatives, support cross-border recognition, and provide a new baseline of trust for regional cooperation on scams and fraud across the wider APAC—helping countries build resilient, verifiable human networks that can withstand the scale and speed of modern online crime

The next section turns to country-level experiences in APAC to consider how PoH might be implemented in practice.

Case Studies: Advanced Technology in Practice

Across Asia, governments have built robust digital identity foundations that verify citizens for public and financial services. Yet most scams occur outside these regulated systems—on social, messaging, and content platforms where anonymity prevails. Emerging Proof of Human (PoH) technologies offer a way to extend the reliability of digital identity into these open environments, confirming humanness and uniqueness without revealing personal data. The following case studies examine how four economies—Japan, South Korea, Malaysia, and the Philippines—are building the elements of PoH-like verification through their national systems, and what lessons their experiences hold for future scam-resilience strategies.

Japan: My Number System and Trust Challenges

Japan's *My Number* system, launched in 2016, assigns a unique 12-digit identifier to every resident for taxation, social security, and disaster-response purposes.[20] Intended to unify administrative data and improve efficiency, it has expanded into the digital realm through the *My Number Card*—a smart ID that enables secure online authentication for e-government services, healthcare, and financial transactions.[21] By 2025, more than 90 million cards—covering over 70 percent of the population—had been issued, though digital usage remains limited due to uneven service integration and persistent trust concerns.[22]

While *My Number* provides verified uniqueness at national scale, it remains a traditional identity system, not a Proof of Human (PoH) framework. Verification is based on government registration and document validation, without the privacy-preserving or cryptographic guarantees that characterize PoH technologies. Nevertheless, Japan's experience demonstrates how state-backed verification of uniqueness can serve as a foundation for extending digital trust and fraud prevention—if coupled with modern, privacy-enhancing mechanisms.

At the same time, Japan's trajectory underscores the limits of centralized identity systems in combating scams. Most online fraud and impersonation occurs in less-regulated environments—social media, messaging, and e-commerce. These platforms operate within general consumer and content regulations, but remain outside Japan's identity-linked assurance mechanisms. Meanwhile, data-handling incidents such as the 2023 mislinked health-insurance records have eroded public confidence and reignited debate over privacy, oversight, and accountability.[23] These episodes illustrate that trust, not technology, remains the binding constraint in expanding verified identity use. Japan's privacy culture—shaped by strong norms around anonymity and cautious attitudes toward state data handling—makes social acceptance a critical factor in deploying any new verification mechanism such as PoH.

In response, the government has introduced stronger governance and interoperability measures, seeking to extend *My Number* Card-based authentication (JPKI) to private-sector domains such as banking, SIM registration, and online commerce.[24] If implemented transparently, Japan could evolve its system into a hybrid digital-trust model—anchoring legal identity in state verification while enabling PoH-style proof of uniqueness through privacy-preserving cryptographic methods. This evolution would allow Japan to link trusted identity with scalable, privacy-respecting verification, strengthening both scam resilience and public confidence in the digital economy.[25]

South Korea: Digital ID Integration and Real-Name Verification

South Korea operates one of the world's most advanced and integrated digital identity ecosystems, built around a national e-ID infrastructure that connects banking, telecommunications, and e-government services.[26] Rooted in the Resident Registration Number (RRN) system introduced in 1968, Korea's identity framework has evolved through layers of real-name verification, biometric authentication, and public-key infrastructure to support its fast-growing online economy.[27] The Digital ID Card (2020) and Mobile Driver's License (2022) marked milestones in transitioning from paper to fully digital credentials.[28] By 2025, more than 50 million Koreans use digital authentication daily—via PASS, Kakao, Naver, or Samsung Pass—to access financial, governmental, and private-sector services.[29]

This deep integration of identity across platforms has been central to Korea's real-name and cybersecurity regime, which requires individuals to verify their legal identity before most online transactions. These mechanisms function as a de facto Proof of Human (PoH) layer, ensuring that digital actors correspond to real, unique individuals and significantly reducing fraud, synthetic identities, and automated abuse. Interoperability between public and private systems has produced high levels of trust and some of the lowest rates of financial-identity fraud globally.[30]

However, Korea's model also reveals the trade-offs of strong centralization. Mandatory real-name rules and data sharing among telecom, financial, and government entities have raised privacy and civil-liberty concerns. Large-scale data breaches, including leaks from credit bureaus and e-commerce platforms, have amplified public skepticism about consent and data minimization.[31] In response, policymakers have strengthened protections under the Personal Information Protection Act (PIPA) and launched a Digital Identity Pilot (2023) exploring user-controlled, decentralized authentication—an important step toward more privacy-preserving models.[32]

Korea's experience demonstrates both the strength and the limits of state-anchored PoH systems. Its combination of verified legal identity, biometric assurance, and interoperable trust frameworks offers a powerful template for scam prevention and digital trust. Yet the Korean debate also highlights growing interest in approaches that offer stronger privacy and user control—principles that align with the direction of emerging Proof of Human (PoH) technologies. As Korea refines its digital-trust architecture, future developments may focus less on strict real-name enforcement and more on balanced models that verify real users while maintaining individual rights and confidence in the digital economy.

Malaysia: MyDigital ID and the Path Toward Biometric Trust

Malaysia's *MyDigital ID* initiative marks a major step toward a unified, state-backed digital identity framework aimed at streamlining access to both public and private services. Launched in 2024 under the Digital Identity Blueprint, the system assigns each resident a biometric-linked digital credential tied to the National Registration Department (NRD) database.[33] Using facial recognition and secure authentication, it allows individuals to verify their identity across e-government portals, banks, telecom operators, and other online services. Early pilots with the Inland Revenue Board (LHDN) and selected financial institutions have laid the groundwork for a full national rollout expected in 2025.[34]

Unlike earlier ID systems, *MyDigital ID* is designed to act as both a credential and verification layer, enabling authentication without repeatedly disclosing personal details. By anchoring identity in a verified biometric record, it provides a foundation for Proof of Human (PoH)-style verification—ensuring that each digital account corresponds to a real, unique individual. As Malaysia expands digital verification across sectors, it faces the same challenge as other economies: extending trust into open, user-driven environments where full identity disclosure is neither practical nor desirable. In this sense, *MyDigital ID* could serve as a backbone for future PoH mechanisms that verify humanness and uniqueness in a privacy-preserving, interoperable way.

The initiative also responds directly to Malaysia's rising exposure to scams and digital fraud, which have increased alongside mobile banking and e-commerce adoption. A trusted identity layer can help reduce impersonation and fake accounts within regulated ecosystems, while PoH-style verification could eventually extend these protections to unregulated spaces—such as online marketplaces, social media, and digital payments—where scams often originate.

The rollout, however, has provoked public debate over privacy, data protection, and governance. Civil-society groups have voiced concern about centralized biometric storage and the potential for misuse if data access is extended beyond its intended purpose.[35] In response, the government has established a Digital ID Steering Committee, reaffirmed compliance with the Personal Data Protection Act (PDPA), and emphasized interoperability with MySejahtera and eKYC systems under Bank Negara Malaysia's oversight.[36] These measures aim to ensure that implementation proceeds with transparency, accountability, and public confidence.

If implemented with clear safeguards and user control, *MyDigital ID* could evolve into a trusted identity foundation for PoH innovation. Its architecture—combining verified biometrics, user consent, and secure interoperability—illustrates how emerging economies can embed verified uniqueness and inclusivity into digital trust frameworks. For Southeast Asia, Malaysia's experience highlights how governance-led identity development can bridge the gap between traditional digital ID systems and future PoH models, reinforcing scam resilience while maintaining privacy and public trust.

Philippines: PhilSys' Rapid Rollout

The *Philippine Identification System (PhilSys)* has become one of the fastest-moving digital identity initiatives in Southeast Asia. Established under Republic Act No. 11055 in 2018, PhilSys assigns each citizen and resident a unique 12-digit PhilSys Number (PSN) supported by biometric data—including facial, fingerprint, and iris scans.[37] Managed by the Philippine Statistics Authority (PSA), the program aims to improve access to public services, promote financial inclusion, and secure digital transactions. By late 2025, over 80 million Filipinos had registered, and the digital version of the ID—available through the eGovPH app and national-id.gov.ph—has gained acceptance across government agencies, banks, and private platforms.[38]

This rapid rollout represents a major milestone in the region's pursuit of trusted identity. By linking verified biometrics to a permanent, unique identifier, *PhilSys* effectively creates a state-anchored proof-of-uniqueness layer, preventing duplicate registrations and synthetic identities. Its integration with financial institutions, telecom operators, and government systems functions as an early, large-scale analogue to Proof of Human (PoH)—confirming that each verified user corresponds to a real, unique individual. The eVerify portal, which allows QR-based credential verification in real time, extends this assurance to digital payments, social protection, and SIM registration.[39]

At the same time, the speed of deployment has brought new governance and privacy challenges. Technical errors, card-production delays, and data-handling issues have drawn public scrutiny, while concerns over centralized biometric storage and opaque data sharing have prompted calls for stronger safeguards.[40] The PSA and National Privacy Commission (NPC) have responded by tightening oversight, adopting stricter encryption standards, and embedding consent-based access protocols within the eGovPH framework.[41]

The Philippine experience illustrates both the promise and risks of rapid digital trust expansion. Its scale and interoperability show how an emerging economy can leapfrog into verified-identity infrastructure that supports financial inclusion and fraud reduction. Yet, the rollout also underscores that trust must evolve alongside technology: public confidence depends on visible accountability, transparent data governance, and user control. As *PhilSys* continues to mature, it offers a valuable testbed for PoH-aligned innovation—demonstrating how verified uniqueness, if paired with strong privacy and inclusion safeguards, can strengthen scam resilience and human-centered trust across Southeast Asia's digital economy.

Case Study Takeaways

Together, these four cases illustrate the divergent pathways through which Asian economies are building proof-of-uniqueness infrastructure. Japan and South Korea demonstrate how advanced regulatory environments can institutionalize verified identity at scale, though with contrasting outcomes: Japan's *My Number* system shows the fragility of public trust when data governance falters, while Korea's real-name regime highlights the efficiency—and risks—of deep integration between identity, finance, and technology. In Southeast Asia, Malaysia's *MyDigital ID* and the Philippines' *PhilSys* reveal two emerging models: one emphasizing careful governance-by-design, the other prioritizing rapid rollout and access. Across all four, a common pattern emerges—PoH-like verification is most effective when coupled with transparency, interoperability, and user control, ensuring that digital identity systems strengthen, rather than erode, public confidence in online safety.

Conclusion and Recommendations

Scams and online fraud have become defining threats to digital trust across the Asia–Pacific region. While national digital ID systems—from Japan's *My Number* to the Philippines' *PhilSys*—have advanced the goal of verified, inclusive identity, they remain primarily administrative tools rather than instruments of real-time fraud prevention. Emerging Proof of Human (PoH) technologies offer a critical complementary layer to these systems: enabling individuals to prove they are unique human users—without revealing personal identifiers—across digital platforms, financial services, and communication networks. By adding a privacy-preserving signal of humanness, PoH can address forms of automated and scaled abuse that traditional digital ID systems were not designed to detect. Integrating PoH into digital identity ecosystems can therefore enhance both resilience against scams and public confidence in digital transactions, while maintaining strong privacy safeguards.

As highlighted in the Safeguards and Governance section, responsible PoH deployment requires risk-based design, clear user protections, and careful alignment with existing identity ecosystems. Building on these principles," governments in the region could:

- **Integrate digital ID and PoH technologies into scam-prevention strategies:** Embed proof-of-uniqueness verification into financial, e-commerce, and communication platforms to reduce impersonation, bot-driven fraud, and synthetic identity risks, while ensuring deployment remains proportionate, low-friction, and aligned with safety frameworks such as ISO/IEC 25389.
- **Support privacy-preserving and interoperable standards:** Encourage the development of regional frameworks that combine biometric assurance with cryptographic privacy protections, ensuring that verified uniqueness does not compromise user anonymity or cross-border usability, and that PoH signals cannot be repurposed for tracking or profiling.
- **Promote regional policy dialogue and coordination:** Leverage existing mechanisms such as the APEC Business Advisory Council, the G20 High-Level Principles for Digital Financial Inclusion, and UN-led digital economy initiatives to align policy objectives, share best practices, and explore pilot frameworks for PoH-enabled verification across sectors, including controlled sandboxes that allow governments and platforms to test PoH in high-risk environments before wider adoption.

Together, these steps would help build a more trusted and human-centered digital ecosystem in Asia—one where verification strengthens security without eroding privacy, where safeguards and governance frameworks ensure responsible use, and where regional collaboration transforms identity systems from administrative registries into active tools for scam resilience and digital inclusion.

Bibliography

[1] Cybersecurity Ventures. n.d. “The World’s Third Largest Economy Has Bad Intentions—And It’s Only Getting Bigger.” Accessed August 2025. https://cybersecurityventures.com/the-worlds-third-largest-economy-has-bad-intentions-and-its-only-getting-bigger/.
[2] Feedzai. 2024. “GASA Global State of Scams Report: $1T Lost to Scams.” Accessed August 2025. https://www.feedzai.com/blog/gasa-global-state-of-scams-report-1t-lost-to-scams/.
[3] GSMA. 2025. *Fraud and Scams Safety Report*. London: GSMA. https://www.gsma.com/solutions-and-impact/connectivity-for-good/public-policy/wp-content/uploads/2025/02/Fraud-and-scams-safety-report.pdf.
[4] UNODC, *Inflection Point: Global Implications of Scam Centres* (2025), p. xx, https://www.unodc.org/roseap/uploads/documents/Publications/2025/Inflection_Point_2025.pdf
[5] Global Initiative, *CRIME CYBER SCAM OPERATIONS IN SOUTHEAST ASIA* (May 2025), https://globalinitiative.net/wp-content/uploads/2025/05/GI-TOC-Compound-crime-Cyber-scam-operations-in-Southeast-Asia-May-2025.pdf
[6] “A New Human Trafficking Trend Emerges from Myanmar,” *The Japan Times*, April 2, 2025, https://www.japantimes.co.jp/news/2025/04/02/japan/crime-legal/myanmar-scam-human-trafficking/
[7] “They were forced to scam others worldwide. Now thousands are detained on the Myanmar border,” *AP News*, March 9, 2025, https://apnews.com/article/myanmar-thailand-scam-centers-trapped-humanitarian-c1cab4785e14f07859ed59c821a72bd2
[8] Signicat. 2024. “Fraud Attempts with Deepfakes Have Increased by 2137% over the Last Three Years.” Accessed August 2025. https://www.signicat.com/press-releases/fraud-attempts-with-deepfakes-have-increased-by-2137-over-the-last-three-year.
[9] CSIS, *Cyber Scamming Goes Global: Unveiling Southeast Asia’s High-Tech Fraud Factories*, December 12, 2024, https://www.csis.org/analysis/cyber-scamming-goes-global-unveiling-southeast-asias-high-tech-fraud-factories
[10] TRM Labs, *The Illicit Crypto Ecosystem Report* (2022), https://www.trmlabs.com/resources/reports/the-illicit-crypto-ecosystem-report-2022.
[11] Meta, “Cracking Down on Organized Crime Behind Scam Centers,” November 21, 2024, https://about.fb.com/news/2024/11/cracking-down-organized-crime-scam-centers/
[12] TRM Labs, 2025 *Crypto Crime Report*, https://www.trmlabs.com/reports-and-whitepapers/2025-crypto-crime-report
[13] World Bank, *Digital Identity Toolkit* (World Bank), section on credential and smart card-based eIDs. https://documents1.worldbank.org/curated/en/147961468203357928/pdf/912490WP0Digit00Box385330B00PUBLIC0.pdf
[14] Financial Action Task Force (FATF), *Guidance on Digital Identity* (Paris: FATF/OECD, March 2020), https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-on-Digital-Identity.pdf (discussion of biometric authentication as part of digital ID assurance).
[15] SITA and PRISM, *Biometric Digital Identity: The Next Step in Seamless Travel and Government Services* (2023), https://www.sita.aero/globalassets/docs/other/biometric-digital-identity-govt-services-prism-report.pdf
[16] OECD, *National Digital Identity (NDID) Platform (Thailand)*, https://www.oecd.org/content/dam/oecd/en/topics/policy-issues/tax-administration/thailand-national-digital-identity-platform.pdf
[17] “Digital Identity Spotlight: Singapore,” 1Kosmos, https://www.1kosmos.com/identity-management/digital-identity-spotlight-singapore/
[18] “Digital identity systems around Asia compared as Taiwan seeks path forward,” *BiometricUpdate*, https://www.biometricupdate.com/202102/digital-identity-systems-around-asia-compared-as-taiwan-seeks-path-forward
[19] Kleros, *Proof of Humanity (PoH) Documentation*, “Proof of Humanity (PoH) is a sybil-resistant registry of humans, combining social verification with video submission to create a trusted list of real humans,” https://docs.kleros.io/products/proof-of-humanity
[20] Government of Japan, *Cabinet Office*, “Outline of the Social Security and Tax Number System (My Number System),” 2016, https://www.cao.go.jp/bangouseido/english/.
[21] Ministry of Internal Affairs and Communications (MIC), “Overview of the Social Security and Tax Number System,” updated 2024.
[22] Digital Agency of Japan, *My Number Card Statistics Portal*, “Number of My Number Cards Issued,” updated October 2025; “Japan’s My Number cards hit 90m issuance but trust issues persist,” *Nikkei Asia*, 12 July 2025.
[23] “Japan suspends some My Number links after health-insurance data mix-up,” *Reuters*, 28 May 2023

[24] "Japan aims to link My Number to banking and SIM registration," *Japan Times*, 9 March 2024.
[25] "Fix the flaws in the My Number system," *Japan Times* (editorial), 2 June 2023; Digital Agency, "Efforts to Enhance Trust in the My Number System," 2024.
[26] Ministry of the Interior and Safety (MOIS), "Overview of the Resident Registration System," Government of the Republic of Korea, 2023.
[27] Korea Communications Commission (KCC), *Real-Name Verification Policy in the Digital Environment*, 2022.
[28] Ministry of Land, Infrastructure and Transport (MOLIT), "Launch of the Mobile Driver's License Service," press release, January 2022.
[29] Korea Internet & Security Agency (KISA), "Status of Digital Authentication Use in Korea," 2024; Yonhap News, "PASS App Surpasses 50 Million Users in Korea," 9 May 2025.
[30] OECD, *Digital Government in Korea: Enabling a Smart and Inclusive Society*, 2023, p. 45.
[31] *Korea JoongAng Daily*, "Massive Data Leaks Raise Questions About Security Practices," 4 February 2023; *Korea Times*, "Credit Bureau Fined over Data Breach Affecting Millions," 15 April 2023.
[32] MOIS, "Digital Identity Pilot Project for Secure Authentication," 2023; Personal Information Protection Commission (PIPC), "Amendments to the Personal Information Protection Act," December 2023.
[33] *Malaysia Digital Economy Blueprint* (MyDIGITAL), Digital Government Division, Ministry of Communications and Digital, "Digital Identity Blueprint," Government of Malaysia, 2024.
[34] Department of National Registration (Jabatan Pendaftaran Negara, JPN), "Implementation of MyDigital ID Pilot with LHDN and Financial Institutions," press release, June 2024.
[35] *Malay Mail*, "Privacy Advocates Raise Concerns over Centralised Biometric Database," 5 April 2024.
[36] Ministry of Communications and Digital (KKD), "Formation of Digital ID Steering Committee," 15 February 2024; Bank Negara Malaysia, *e-KYC* Implementation Guidelines, revised 2023.
[37] Republic Act No. 11055, "An Act Establishing the Philippine Identification System (PhilSys Act)," Official Gazette of the Republic of the Philippines, August 2018.
[38] Philippine Statistics Authority (PSA), *PhilSys Dashboard: Registration and Issuance Data*, updated October 2025; *Inquirer.net,* "Over 80 Million Filipinos Registered for National ID—PSA," 14 September 2025.
[39] PSA, "PhilSys eVerify Portal Launch and QR Verification Capabilities," 2024.
[40] *Rappler*, "Privacy Concerns Mount over National ID Data Sharing," 22 June 2024; *Philippine Star*, "National ID Delays, Data Glitches Spur Criticism," 10 May 2024.
[41] National Privacy Commission (NPC), "NPC Advisory on Data Protection Standards for the National ID System," 2024; PSA, "Enhanced Security Measures for ePhilID Rollout," 2024.

www.seapublicpolicy.org