RESEARCH INSIGHTS

WINNING THE WAR ON DEEPFAKES

ASEAN FINTECH FORUM

ASEAN ECONOMIC FORUM

Sabio

Photos taken from Unsplash.com, and iStock. Cover Image contributed by 8machine via Unsplash.com. Image contributions by Carolin Thiergart, Logan Voss, Pawel Czerwinski, Resource Database, Ihon Karwan

Key Takeaways

1

AI-Fueled Deepfakes Are Undermining Trust

Sophisticated impersonation attacks are exploiting human trust in voice and video, leading to major financial losses and identity breaches across Southeast Asia.

2

Identity Is Now the Prime Target

Fraud is shifting from technical vulnerabilities to identity manipulation, requiring institutions to adopt layered defences like biometric checks and digital ID wallets.

3

Public Awareness Is Crucial

Low digital literacy, especially among the unbanked, makes populations highly vulnerable. Scams must be countered with targeted, ongoing public education.

4

Collaboration Must Cross Borders

Tackling AI fraud requires ASEAN-wide cooperation; shared data, common frameworks, and synchronized regulatory actions are essential for resilience.

5

People Remain the Weakest Link

Human error continues to be a key vulnerability. Building a cyber-aware workforce through training and behavioural monitoring is critical to long-term defence.

The Erosion of Trust in a Synthetic World

In a collaborative effort between the ASEAN Fintech Forum and Sabio Research, a senior-level research roundtable was held in Indonesia to explore deepfakes in the era of AI.

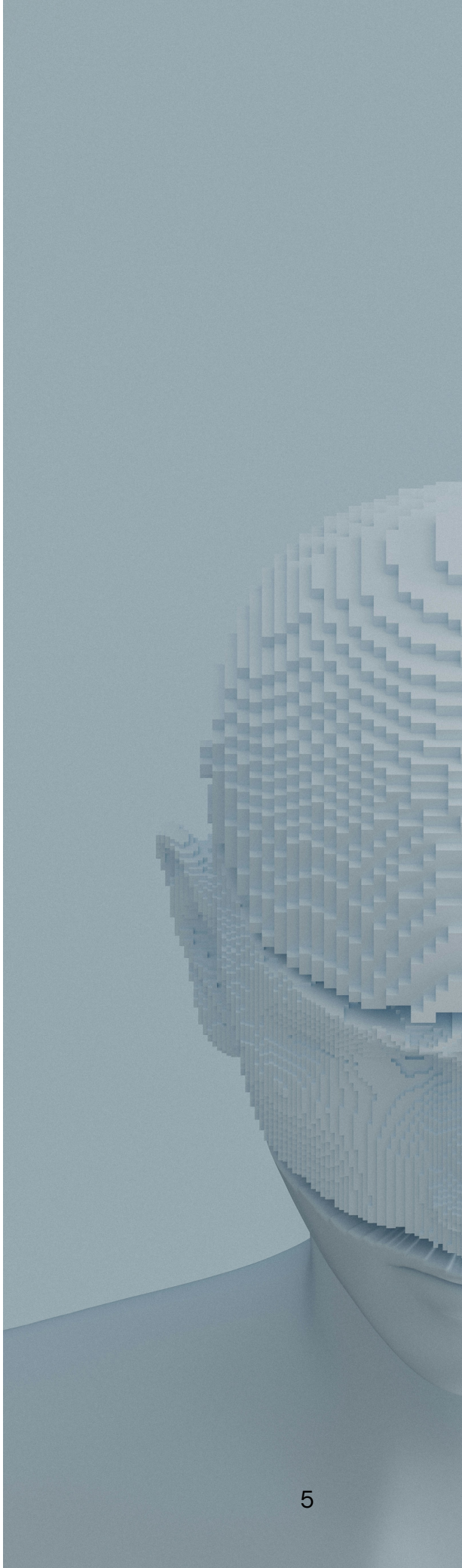
The roundtable began with a stark acknowledgment: what we see and hear can no longer be trusted. Deepfakes have become cheaper, more realistic, and accessible to both lone actors and well-funded criminal networks. Sophisticated fraud campaigns now target individuals with tailored impersonations, often orchestrated over video conferencing tools and social media. These threats are not hypothetical; they've already resulted in multimillion-dollar financial losses across the region.

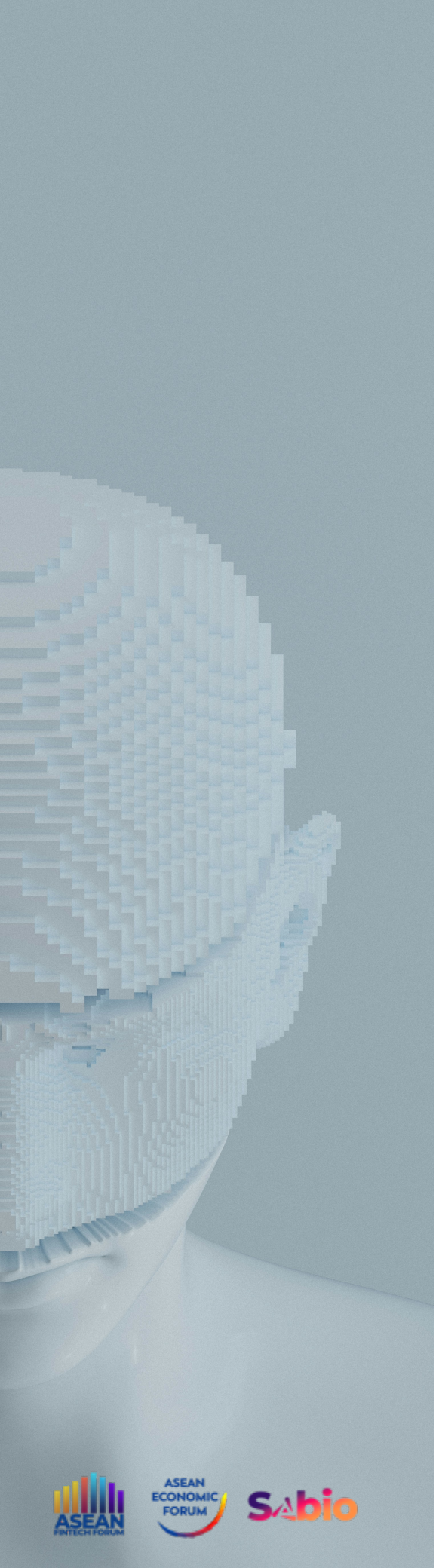
This growing crisis stems from a fundamental vulnerability: our identities, once authenticated through basic credentials or visual cues, are now easily forged. From CFOs receiving urgent (but fake) video calls from supposed CEOs to family members being tricked by cloned voices of loved ones, the lines between real and fake are dangerously blurred.

Identity as the New Battlefield

With fraud shifting from technical exploits to identity manipulation, the industry has been forced to rethink its defense posture. Traditional authentication methods like OTPs are being phased out, deemed insufficient in an era where even voice and facial biometrics can be mimicked. In response, leading institutions are now layering their defenses with adaptive authentication, liveness detection, biometric match checks, and the adoption of digital identity wallets.

Digital platforms in Indonesia and Thailand, for instance, are implementing stricter onboarding mechanisms that cross-reference user-submitted identity data against existing databases. AI-powered facial matching and fraud pattern recognition are helping to filter out synthetic or duplicated identities. However, this requires ongoing investment; not just in tools, but in talent and system design.





Public Vulnerability and the Call for Education

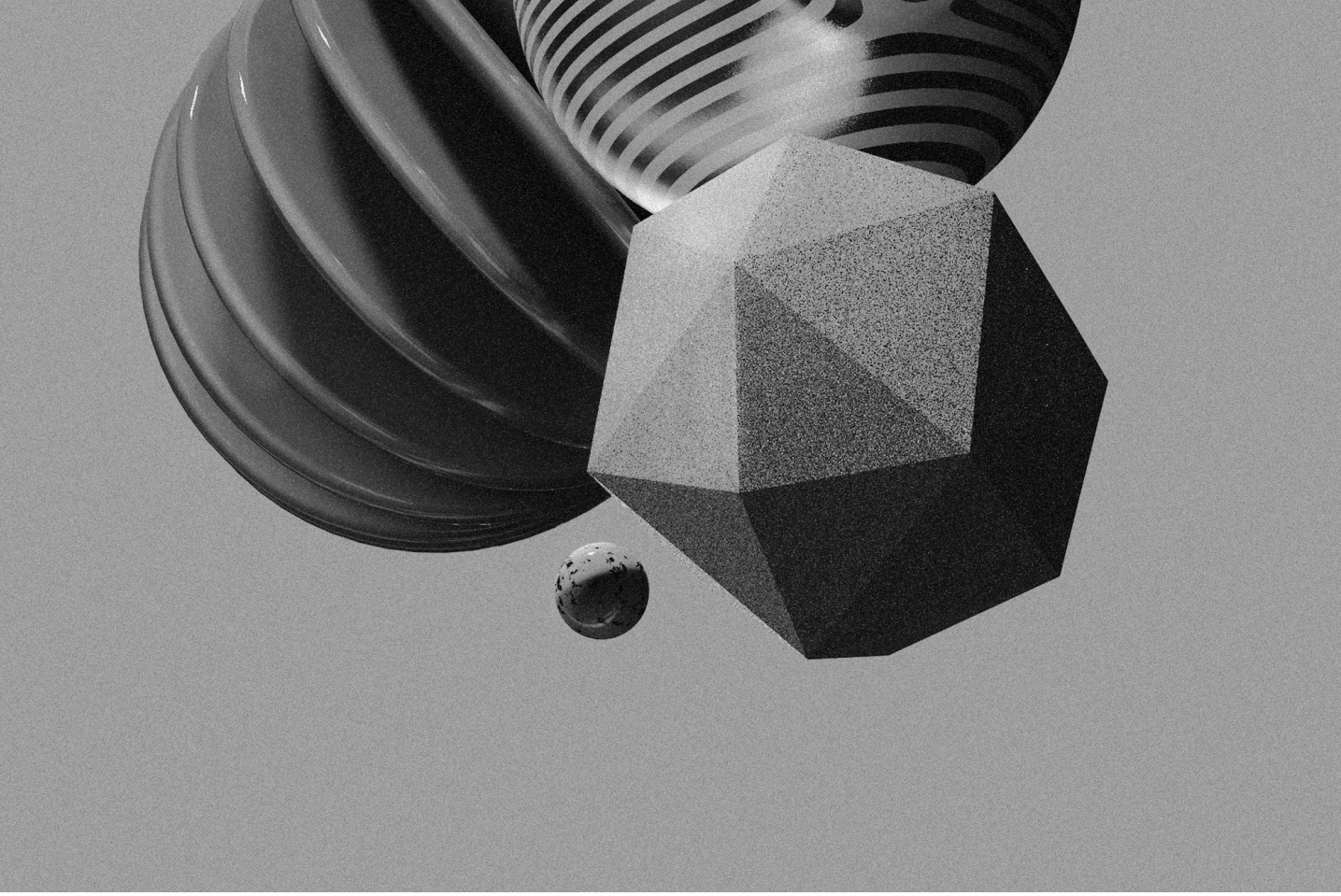
Even as systems become smarter, a large portion of Southeast Asia's population, particularly the underserved and unbanked, remains highly vulnerable to AI-powered scams. The instinct to trust familiar voices and faces, combined with limited digital literacy, makes them easy targets for voice-cloning and phishing schemes.

To address this, several financial service providers have launched wide-reaching education campaigns, using mobile apps, social media, and national broadcasts to build public awareness. These efforts aim to instill caution in users and reinforce good digital hygiene practices. Education is no longer a CSR initiative; it is a frontline defense strategy.

Cross-Sector and Regional Collaboration Are Imperative

Recognizing that no single institution can tackle AI fraud in isolation, participants emphasized the need for industry-wide collaboration and regulatory alignment. In the Philippines and Singapore, private-public initiatives are already underway, with fraud bureaus being formed to share intelligence and blacklist fraudulent accounts. Some jurisdictions are also enforcing SMS link bans and mandating friction layers in payment transfers to intercept suspicious behavior.

However, the discussion revealed gaps at the ASEAN level. Without harmonized regulation, efforts remain fragmented. Participants called for regional data-sharing agreements, common digital identity frameworks, and joint enforcement mechanisms to create a resilient and interoperable trust ecosystem.



Cybercrime as Industry: Fighting an Asymmetrical War

A sobering realization emerged throughout the dialogue; cybercrime is no longer opportunistic; it operates like a business. Fraud rings today possess the R&D, funding, and strategic agility of formal enterprises. They exploit technology faster than regulators can respond and often work across borders with seamless digital coordination.

Financial institutions, on the other hand, must navigate compliance, system rigidity, and legacy infrastructure. This asymmetry puts defenders in a constant reactive posture. To shift this dynamic, organizations are now investing in proactive fraud prevention, cyber threat intelligence, and behavioral analytics, targeting not just external actors, but also internal vulnerabilities.

The Human Element: The Last (and Weakest) Line of Defense

Despite advanced tools, one consistent challenge remains: human behavior. Whether it's an employee clicking a malicious link or a staff member inadvertently bypassing protocol, many breaches ultimately trace back to lapses in judgment or awareness. Financial institutions are now exploring behavioral profiling and employee risk scoring to flag individuals who may be susceptible to manipulation, due to stress, financial pressure, or negligence.

Reducing the human attack surface doesn't mean removing people from the equation, but it does require a cultural shift. Continuous training, tighter hiring practices, and fostering a cyber-aware workforce are all becoming essential pillars of modern fraud resilience.

Conclusion: Building a Trusted Digital Future

The roundtable closed with a shared understanding: identity is no longer just a security concern; it is the cornerstone of digital trust. As AI continues to reshape the threat landscape, financial institutions must invest not only in robust technology but in people, education, and cross-sector collaboration.

AN INDUSTRY CALL TO ACTION :

- A renewed push for multi-factor, adaptive verification as standard practice.
- Stronger regional cooperation on data and regulatory harmonization.
- The formalization of fraud intelligence-sharing networks.
- Scaling public education efforts across digital channels.
- Prioritizing human behavior monitoring and workforce resilience.

In this new era, only the verified can be trusted; whether human, machine, or AI agent. The path forward lies in building systems and societies that are not only secure, but also smart, inclusive, and vigilant.