

Scene-Setting Remarks on Digital Safety
Deputy Governor Daranee Saeju
World Economic Forum at the IMF-WBG Annual Meetings
15 October 2026

Good afternoon, distinguished guests and WEF colleagues.

My sincere appreciation to the World Economic Forum for convening us today.

I have chosen **digital safety** as today's focus because the issue has never been more timely. As digital finance becomes faster, more connected and more widely used, fraud is evolving just as quickly – putting not only people's money at risk, but also their **trust in the financial system**.

I. Why Safe and Inclusive Digital Finance (SIDF)

For the Bank of Thailand, **safety and inclusion must therefore advance together**: access is only meaningful when people feel protected and confident using digital financial services. This is at the heart of the **Safe and Inclusive Digital Finance agenda** that we are promoting.

We have made real progress in digital finance. It has lowered costs, sped up payments, and brought millions of people into the financial system. In Thailand, **PromptPay**, our instant payment system, now handles more than **80 million transactions** a day – almost 10 times the 2019 level. In **value** terms, the system processes nearly **5 trillion baht a month** – 16 times higher the 2019 level. **Annually, transaction value** reached **54 trillion baht in 2025** – more than twice the size of Thailand's GDP.

Yet protection has not kept pace with innovation. Fraudsters exploit instant, interconnected systems to move stolen funds across institutions and borders before the ecosystem can intervene.

The consequences are growing. Globally, **fraud and scams cost an estimated 579 billion US dollars in 2025 alone**, and the FATF reports that 90 percent of jurisdictions view fraud as a major money-laundering threat. Fraud is therefore no longer only a consumer protection issue; it is a threat to trust and, ultimately, financial stability.

That gap is why Thailand, as host of the Annual Meetings, partnered with the IMF and World Bank Group to develop the **Bangkok Blueprint for Fraud-Resilient Financial Services**. The Blueprint serves three related ambitions. First, as a **practical policy reference**; Second, as a **catalyst for global collaboration**; And finally as a **foundation for standard setters** to build on.

II. The Blueprint in Action: From regional to global

The Blueprint brings the **Safe and Inclusive Digital Finance agenda** to life – turning the concept into a tangible and practical basis for further global collaboration. Launched yesterday with its companion paper, *The Bangkok Blueprint in Action*, it combines Key Considerations with lessons from Thailand, Hong Kong, Malaysia and Singapore – showing what works, where trade-offs arise, and how principles can become action.

III. WEF-BOT Workshop: Whole-of-ecosystem Approach in Action

Inspired by the Blueprint's whole-of-ecosystem approach, our July workshop with the WEF brought together participants across regions and sectors to test its Key Considerations. One insight stood out: **the threat is integrated, but our response remains fragmented.**

Closing that gap requires each actor to contribute its capabilities, innovation to connect those efforts, and trust and safety to be treated as shared infrastructure.

The Bangkok Blueprint is a whole-of-ecosystem answer: it helps us see and act across the whole track. **Its Key Considerations** provide a common basis for financial institutions, technology and telecommunications firms, online platforms, regulators and law enforcement to align roles, share intelligence and innovate together.

One powerful message from the workshop is that “**criminals collaborate by default, so our response must collaborate by design**”. By carrying this approach across sectors and borders, and translating regional experience into adaptable principles, the Blueprint can help move the global community from fragmented efforts to coordinated action.

IV. From Principles to Practice

Thailand's experience helped shape this approach. Our Emergency Decree on Technology Crime enables real-time information sharing across banks, telecoms, digital asset operators and online platforms. With shared systems like our Central Fraud Registry, a single fraud report can trigger tracing, account suspension and law-enforcement coordination.

For the past year and a half, we have not recorded a single unauthorized mobile banking transaction caused by money malware. **However, criminals adapt.** They no longer need to break into the phone. They only need to convince the person holding it **to authorize the payment.**

This brings us to today's question: can the AI behind fraud also help us fight it? Yes, but only if we use it together. AI can identify suspicious behavior, uncover hidden mule-account networks, and detect threats earlier. But it must be secure by design, transparent, accountable, and ultimately serves the public.

V. Closing: The Work Ahead

What I have outlined today makes clear that much more remains to be done. The Blueprint is not an endpoint, but a starting point to spark deeper dialogue and stronger collaboration across sectors and borders. Turning that momentum into action raises three questions for this session.

First, how do we turn AI from the fraudster's weapon into our best defense, and when AI agents move money for us, who is accountable? **Second**, what collaboration would let intelligence move as fast as the money? **And third**, as we tighten controls, how do we keep people protected, not pushed out?

With that, let me hand over to our moderator.

Thank you.