TRANSNATIONAL BANKING CRIME

Indonesia's Regulatory Architecture, New Code, and Recommendations for Discussion

Indonesia's Architecture
OJK, PPATK & the legal framework

Indonesia's New Code
KUHP, KUHAP & corporate liability

Recommendations
Suggestions for discussion

THE PRESIDENTS OF LAW ASSOCIATIONS IN ASIA (POLA) 2026 · 8 September 2026

Almaida Askandar, S.H., MBA

Pullman Thamrin, Jakarta, Indonesia.



Scope of Today's Discussion

Indonesia's regulatory architecture, its new criminal code, and recommendations for discussion

01 Indonesia's Architecture

The regulatory and institutional chain that handles a banking-crime case inside Indonesia — OJK, PPATK, Bareskrim Polri, and the Attorney General's Office — and the law that governs each stage.

02 Indonesia's New Code

What the new Criminal Code (KUHP) and Criminal Procedure Code (KUHAP) change — corporate liability, sentencing, electronic evidence, restorative justice, and deferred prosecution.

03 Suggestions for Discussion

Practical recommendations for regulators, law enforcement, and the legislature — closing the gaps this framework still leaves open in cross-border banking cases.



Indonesia's Regulatory Architecture in Transnational Banking Crime

The procedural sequence a cross-border case actually follows — detection, investigation, trial, then cross-border recovery — and the law governing each stage

1 PREVENTION & DETECTION

Also: bank, police

AML / CFT Obligations

CDD, EDD, and suspicious-transaction reporting duties for financial institutions.
OJK = Financial Services Authority

POJK No. 8 of 2023

Anti-Money Laundering Law

Predicate offences, STR filing, and PPATK's mandate as the financial intelligence unit.
PPATK = Financial Transaction Reports and Analysis Center

Law No. 8 of 2010

2 INVESTIGATION

OJK Law, as amended by P2SK

Legal basis for OJK's investigative authority across the whole financial sector.

Law No. 21/2011 jo. Law No. 4/2023

Investigation of Financial-Sector Offences

Scope of offences (Art. 2); investigator powers; violation-settlement route.

POJK No. 16 of 2023

3 THE OFFENCE & TRIAL

Criminal Code (KUHP)

Jurisdiction (Arts. 4–7); corporate liability (Arts. 45–50); Art. 187 binds sectoral statutes.

Law No. 1 of 2023

Criminal Procedure Code (KUHAP)

Electronic evidence (Arts. 235(1)(f), 242); RJ (Arts. 79–88) barred ≥5-yr terms.

Law No. 20 of 2025

Banking Law

Art. 49(1)(a) & 49(2) — the core offence-creating provision.

Law No. 7/1992 jo. Law No. 4/2023

4 CROSS-BORDER COOPERATION

Mutual Legal Assistance

Assistance (Art. 3); refusal grounds (Art. 6); foreign confiscation orders (Arts. 51–53).

Law No. 1 of 2006

Extradition

Diplomatic request (Art. 22); court determination (Arts. 26–27); presidential decision (Art. 36).

Law No. 1 of 1979

Institutional roles across this sequence: OJK leads investigation, PPATK supplies financial intelligence, Bareskrim Polri applies coercive powers, and the Attorney General's Office prosecutes and pursues cross-border recovery.

Two Global Conventions on Cybercrime

Council of Europe, 2001 · Guides 50 countries

Budapest Convention on Cybercrime

The first international convention on cybercrime, aimed at strengthening international cooperation against it. It guides national cybercrime regulation in 50 countries, including the United States, Australia, and Japan — Indonesia is an observer, not a party. The Convention recognizes two categories of cybercrime: offences against the confidentiality, integrity and availability of computer data and systems (e.g. illegal access, system interference), and computer-related offences, where a computer is the tool for another crime (e.g. online banking fraud for financial gain).

United Nations, adopted December 2024 · Guides 75 countries

UN Convention on Cybercrime

The first global cybercrime treaty under UN auspices, adopted by the UN General Assembly in December 2024. It guides 75 countries, including the UK, China, and Thailand — Indonesia is a committee member. It covers illegal access and illegal interception, offences related to online child sexual abuse, and non-consensual dissemination of intimate images. Article 35 commits state parties to cooperate as widely as possible on investigation, prosecution and judicial proceedings for cybercrime, and on collecting electronic evidence for the offences it covers and for any other serious crime carrying a minimum four-year penalty.



What this means for Indonesia Neither treaty binds Indonesia as a full party today — Indonesia is an observer at Budapest and a committee member at the UN table. Domestic reach into cross-border cybercrime instead runs through Article 4 of the new Criminal Code, the Mutual Legal Assistance Law, and the Extradition Law.

Sources *Council of Europe, Budapest Convention on Cybercrime (2001); United Nations General Assembly, UN Convention against Cybercrime (adopted December 2024), Art. 35. Country and status counts as presented in Webinar IABF, 15 April 2026.*

Corporate Liability and Sentencing Under the New Code

The Corporation as a Criminal Subject

A corporation may be held criminally responsible for offences committed for it, on its behalf, or in its interest — reaching management, employees, and persons in a working relationship with it. Liability can attach to the corporation, to the persons who control it in fact, or to both, and follows the entity through merger, acquisition and restructuring.

ARTICLES 45–50

Sanctions: Fines and Beyond

Fines are the principal penalty, aggravated where the offence produced substantial gain — materially heavier than under the old Code. Additional sanctions: compensation, restoration of the offence's consequences, publication of the judgment, supervision, suspension of business, revocation of licence, and dissolution.

ARTICLES 119 - 124

Purpose of Punishment and Sentencing

Punishment is no longer retribution alone: the Code names prevention, rehabilitation, resolving the conflict, restoring the balance disturbed, and a sense of security as its aims. The court weighs the offender's fault, motive and conduct after the offence, the loss caused, and the victim's own account and forgiveness.

ARTICLES 51–55

Judicial Pardon and Restoration

The court may find guilt established and still decline to punish, having regard to the slightness of the act, the offender's circumstances, and justice and humanity (Art. 54(2)). Compensation and restoration may also be imposed as additional penalties — restoration becomes part of the sentence, not a separate civil claim.

ARTICLE 54(2)

AND THE OFFENCE ITSELF The offence-creating provision remains Article 49(1)(a) and 49(2) of the Banking Law (Law No. 7 of 1992, as amended by Law No. 4 of 2023). Judicial pardon under Art. 54(2) is discretionary and case-by-case — not a categorical route out of trial. For the Procedure Code's restorative-justice and deferred-prosecution mechanisms.

AND ITS REACH ACROSS BORDERS Article 4 of the Code extends Indonesian jurisdiction to offences committed within Indonesian territory, aboard an Indonesian vessel or aircraft, or — under Art. 4(c) — in the field of information technology or any other offence whose effects are experienced or occur within Indonesia. That third limb is the statutory basis for prosecuting borderless cybercrime and transnational offences under Indonesian law wherever their impact lands here.

Evidence, Diversion, and Cross-Border Cooperation Under the New Code

Electronic Evidence and Digital Forensics

Electronic evidence is now its own category of lawful evidence — transaction logs, device data, exchange records, communications — alongside testimony and documents. The investigator may obtain digital forensic assistance and call on expert institutions; authentication itself is not mandated, only made available.

ARTICLES 235(1)(f), 242, 55–56

Restorative Justice: Threshold and Termination

The offender and victim may agree on restoration — apology, return of property, or compensation — performed within seven days and available at investigation, prosecution, and trial. Only a first offence carrying ≤5 years qualifies; state-security, terrorism, corruption and sexual-violence offences are excluded.

ARTICLES 79–88, 80(1), 82

Deferred Prosecution Agreements

A court-approved DPA lets the prosecutor suspend a corporation's prosecution, subject to compliance conditions and the court's ratification.

ARTICLE 328(1)–(17)

Cross-Border Evidence and Cooperation

Electronic-evidence rules reach records held abroad, but cross-border requests still run through the MLA Law and the Extradition Law — not a standalone regime of their own.

ART. 235(1)(f) CF. LAW NO. 1/2006, LAW NO. 1/1979

How a DPA Differs from Restorative Justice

RJ is available from the investigation stage for any first offence carrying ≤5 years, and needs both victim and accused to agree. A DPA is corporate-only, arises once the prosecution phase begins, needs the prosecutor's and the court's approval — and is not capped at RJ's 5-year ceiling.

ART. 328 CF. ARTICLES 79–88

What This Means for a Cross-Border Case

A domestic case can resolve early through OJK's settlement route, a DPA, or restorative justice. But once assets or the suspect leave Indonesia, resolution depends on the 2006 MLA Law and the 1979 Extradition Law — neither DPA nor RJ yet has a cross-border counterpart.

THE PRACTICAL GAP

The two largest gaps for a cross-border case: authentication of electronic evidence is left to the trial judge with no prescribed standard, and neither the DPA nor restorative justice extends across a border — recovery of assets or the person abroad still depends entirely on the 2006 MLA Law and the 1979 Extradition Law. Both return in the recommendations.

When Is a Bank Liable for a Customer's Loss?

System failure or internal bank negligence

When the Bank Is Liable

A bank must be liable — including paying compensation — where a customer's loss stems from a system failure or the bank's own internal negligence: a breach of the bank's central database that wipes customer balances or leaks card data; an employee who misuses access to customer data for illegal transactions (an inside job); ATM skimming the bank enabled by failing to install anti-skimming devices or inspect machine security; or a failure to deliver a valid transaction or OTP notification, letting an illegal transaction proceed unnoticed.

Customer's own fault — the 'user negligence' principle

When the Bank Is Not Liable

Under the 'user negligence' principle, a bank is released from liability where the loss stems from the customer's own error: social engineering, where the customer hands an OTP, PIN or password to someone posing as a bank employee by phone or text; a lost phone not promptly blocked, or an unofficial app that lets malware take over mobile banking; a transaction authenticated correctly (valid multi-factor authentication) is treated as the customer's own unless they can prove the bank's system itself was breached; or the customer knowingly shares account or card access with family or a third party.

Why this matters The line drawn here is exactly what decides liability in the cases that follow — a bank is not liable where the loss traces to the counterparty's own systems or the customer's own mistake, not the bank's. Every case study in this deck turns on which side of this line the facts fall.

Sources *Law No. 4 of 2023 on the Development and Strengthening of the Financial Sector, Art. 236(3); Law No. 8 of 1999 on Consumer Protection, Arts. 4 and 7; Law No. 21 of 2011 on the Financial Services Authority (OJK), Art. 4. Presented in Webinar IABF, 15 April 2026.*



CASE STUDY ONE · REPORTED 2025, STILL UNDER INVESTIGATION

Internal Systems - Intrusion in one of Indonesian Bank

Jun 2024 – Mar 2025

The Intrusion

Over some ten months a syndicate is reported to have exploited weaknesses in the internal applications and third-party middleware of eight participating banks. Central Bank of Indonesia **("BI")**'s own review traced the source to the victim bank's internal application, not to infrastructure the central bank manages.

29 Mar 2025

The Largest Single Loss

Between 11 and 11.20 AM Jakarta Time, the victim Bank recorded some 807 transactions draining approximately IDR 227–228 billion from the settlement account it maintained for BI-FAST. Across the eight banks the reported aggregate approaches IDR 800 billion.

Within Hours

Layering and Exit

Proceeds were routed through collection accounts opened in the names of local individuals and converted into crypto assets on international exchanges. Reported traces of access point to Taiwan, mainland China, Hong Kong and Cambodia.

Nov 2025 Onward

BI Confirms: Not a BI-FAST Breach

BI has confirmed the anomalous transactions did not originate from the BI-FAST system, and says BI-FAST itself continues to meet international security standards. BI is coordinating with OJK and law enforcement on recovery, and has reminded participating banks to strengthen internal security. PPATK froze related accounts; by November 2025 Polri had named six suspects tied to the collection accounts and transfer facilities used to move and convert the funds. The individuals who breached the banks' systems have not been identified, and the investigation continues.

What the case shows Attribution matters here as much as speed: this was a breach of one bank's own application layer, not of shared payment infrastructure — a distinction BI moved quickly to draw, and one that shapes who is liable. Every domestic stage engaged fast: detection, blocking, freezing, and the naming of suspects on the money trail. Cross-border cooperation has produced nothing — and not for want of treaties. Indonesia has MLA with China (Law No. 8/2006) and Hong Kong SAR (Law No. 3/2012), extradition with both (Law No. 13/2017; Law No. 1/2001), and MLA with Cambodia under the ASEAN Treaty (Law No. 15/2008). Only Taiwan sits outside every channel. The gap is speed, not coverage: the money reached foreign exchanges in hours; an MLA request runs in months.

Phishing Cases
Business Email Compromise and Wire Diversion: Two Private-Sector Cases

UK Buyer × Japanese-Owned Investment Company (PT PMA, Indonesia)

Case #2 — Settled by Private Agreement

In a machinery sale between a UK buyer and an Indonesian PT PMA (foreign-owned by a Japanese parent) as seller, a hacker breached the seller's email and sent the buyer fraudulent payment instructions under the seller's name, redirecting funds to the attacker's account — a classic business email compromise. The seller never received payment; by the time the fraud surfaced, the funds in the attacker's account had already been withdrawn, and the bank could not be held liable. The parties treated the loss as an external event outside either side's control: under a settlement agreement, the buyer repaid 50% of the transaction value, and the seller withdrew the police report it had filed against the buyer.

Swedish Producer × Indonesian Recipient Bank

Case #3 — Recovered Through the Courts

A Swedish producer never received payment for a cross-border sale; tracing showed the funds had been diverted mid-transfer into an unrelated Indonesian bank account, indicating interception or fraud. Because the funds had not yet been withdrawn, the producer reported the matter to Bareskrim Polri, which froze the recipient account, and separately petitioned the East Jakarta District Court for a declaration that the funds were unlawfully received. The petition succeeded, and the bank was ordered to return the full amount to the producer.

What the case shows Timing decided the outcome. Case One's funds moved before the fraud was discovered, so recovery came only through a private settlement at half value. Case Two's funds hadn't yet been withdrawn, so a police freeze plus a civil unjust-enrichment petition recovered the money in full — the same exposure, resolved two different ways by how fast each victim moved.

Sources *IABF Law Group, client case files presented at Webinar IABF (15 April 2026), summarized and anonymized. Figures, dates and legal characterizations are as presented in that webinar; the underlying matters are private disputes and not court-published decisions.*

What Three Cases Teach About Cross-Border Fraud

1 TIMING

Speed Decides the Remedy

Funds not yet withdrawn can be frozen and recovered in full — IABF Case Two's civil petition succeeded, and PPATK's freezes did the same for the victim Bank, because the money hadn't moved. Once it has, recovery is partial at best, as IABF Case One's 50% settlement shows.

2 ATTRIBUTION

Whose System Failed Decides Who Pays

BI moved quickly to confirm the victim Bank breach sat in the victim bank's own application, not shared infrastructure — and in both IABF cases the bank was not held liable, because the breach or interception happened between the private parties, not inside the bank.

3 FORUM CHOICE

Civil Remedies Can Outpace Criminal Process

IABF Case Two recovered the full amount through a police freeze and a civil unjust-enrichment petition to the district court — faster than waiting on a criminal conviction, and a track worth teaching alongside the criminal-procedure route this framework centers on.

4 PRIVATE ORDERING

Settlement Is a Real, Imperfect Track

IABF Case One shows commercial counterparties often resolve a cross-border fraud by private agreement rather than litigate it to conclusion — at a discount to the loss, and off the public record this framework otherwise assumes.

5 CROSS-BORDER SPEED

The Money Outruns the Law

The victim Bank's proceeds reached foreign exchanges within hours; both IABF cases moved money across a border in a single transfer. Our domestic procedure engages fast, but— cross-border recovery — are where all three cases got stuck, or had to route around the treaty machinery entirely.

Three cases, one pattern: whoever moves first — freezing an account, filing a civil petition, or negotiating a settlement — recovers something. Whoever waits on the formal channel recovers nothing at all, or arrives after the money is already gone.

CURRENT DATA · AS OF 31 AUGUST 2026

Indonesia's Anti-Scam Enforcement, in Numbers

Satgas PASTI and IASC form the domestic detection layer; FRONTIER+ is Indonesia's first real-time cross-border anti-scam network

1

Satgas PASTI — Illegal Financial Activities Task Force

25,875

illegal-entity complaints received, 1 Jan – 31 Jul 2026

22,529 involved illegal online lending, 3,170 illegal investment schemes, and 176 illegal pawn services — the three modi Satgas PASTI tracks most closely.

OJK PRESS RELEASE, 31 AUG 2026

2

Indonesia Anti-Scam Centre (IASC)

637,055

scam reports received, 22 Nov 2024 – 31 Jul 2026

1,179,881 accounts reported and verified, of which 607,210 have been blocked. Cross-agency coordination has frozen roughly Rp724.1 billion in scam-related funds and returned Rp204.3 billion to victims.

OJK PRESS RELEASE, 31 AUG 2026

3

FRONTIER+ Cross-Border Platform

14 jurisdictions

real-time anti-scam intelligence network, incl. Indonesia

Operation FRONTIER+ (10 Mar – 7 May 2026) deployed over 3,200 personnel across 9 authorities: 3,018 arrests, about 102,000 accounts frozen, and over US$161m (~Rp2.83tn) recovered of US$752m (~Rp13.2tn) in reported losses.

OJK PRESS RELEASE, 25 MAY 2026

Sources *OJK, 'Satgas PASTI Terima 25 Ribu Pengaduan Aktivitas Keuangan Ilegal dan IASC Berhasil Blokir Dana Terkait Scam Rp724 Miliar' (SP 16/STPASTI/VIII/2026, 31 Aug 2026); OJK, 'Indonesia Anti-Scam Centre Gelar Operasi Bersama Penanganan Penipuan Lintas Negara' (SP 07/STPASTI/V/2026, 25 May 2026). Figures as reported by OJK; both matters remain under ongoing operation.*

Stopping Transnational Banking Crime

To combat cross-border financial crime, global authorities and financial institutions must focus on unified tracking systems, real-time intelligence sharing, and stringent regulatory enforcement.

1 Harmonize Global AML/CFT Regulations

Standardize Anti-Money Laundering (AML) and Counter-Financing of Terrorism (CFT) laws across jurisdictions to eliminate regulatory havens.

2 Deploy AI-Driven Transaction Monitoring

Utilize centralized, machine-learning systems to detect anomalous, cross-border wire patterns instantly.

3 Mandate Beneficial Ownership Transparency

Require all countries to maintain public, verifiable registries of the true owners of corporate entities and trusts.

4 Establish Instant Cross-Border Intelligence Loops

Create secure, automated data-sharing pipelines between international Financial Intelligence Units (FIUs).

5 Sanction Non-Compliant Offshore Jurisdictions

Impose strict economic penalties and banking restrictions on nations refusing to comply with international financial policing standards.

6 Standardize Crypto Asset Tracking

Enforce the Financial Action Task Force (FATF) 'Travel Rule' globally to trace digital asset movements across sovereign borders.

AND TRAIN THE PEOPLE, NOT JUST THE SYSTEM Regulations and technology close the gaps in the system, but every case in this deck turned on a person — a compromised email, a trusting customer, a recruited mule. Fund and require regular, realistic cybersecurity education and training for bank staff and the public, so the human element stops being the easiest way in.

NOTES: Indonesia is targeting the enactment of the Asset Forfeiture Law in December 2026 to reinforce the legal framework governing the tracing, freezing, and seizure of assets and facilitate the recovery of proceeds associated with economically motivated crimes.

Recommendations for Lawyer Associations

Simple, practical steps a lawyer association can actually carry out — to keep members from inadvertently or deliberately facilitating illicit financial flows.

1 Implement Mandatory KYC Training

Require annual continuing legal education (CLE) credits focused on Know-Your-Customer (KYC) and customer due diligence protocols.

2 Publish a Client Due-Diligence Checklist

Give members a short, standard checklist for verifying a client's identity and source of funds before opening a matter — a practical reference they will actually use.

3 Enforce the Rules Already on the Books

Apply the Bar's existing disciplinary rules consistently: a lawyer who knowingly helps set up a fraudulent corporate structure should face real consequences, not just a warning.

4 Require Routine Cybercrime Education and Integrity

Give members regular, updated training on cybercrime typologies and cross-border fraud schemes. A lawyer's integrity is non-negotiable — no member may knowingly assist, structure, or shield a client's involvement in cybercrime.

Thank you

Almaida Askandar, S.H., MBA

POLA 2026 · Transnational Banking Crime

IABF LAW GROUP

Intiland Tower, 9th Floor
Jalan Jenderal Sudirman No. 32
Jakarta 10220, Indonesia

mail@iab-net.com · **almaida@iab-net.com**

GLOBAL NETWORK

IABF Law Group is the Indonesia member firm of ALFA International, the premier global network of independent law firms — 140+ member firms across 80+ countries, since 1980.

alfainternational.com