

Republic of the Philippines
HOUSE OF REPRESENTATIVES
Quezon City

TWENTIETH CONGRESS
Second Regular Session

HOUSE BILL NO. 11333



Introduced by: Hon. Keith Micah "Atty. Mike" D.L. Tan

AN ACT

ESTABLISHING AN EMERGENCY FINANCIAL ACCOUNT BLOCKING MECHANISM FOR LOST, STOLEN, OR COMPROMISED MOBILE DEVICES, PROTECTING CONSUMERS FROM UNAUTHORIZED DIGITAL FINANCIAL TRANSACTIONS, PRESCRIBING OBLIGATIONS OF FINANCIAL SERVICE PROVIDERS AND OTHER COVERED ENTITIES, AND PROVIDING PENALTIES THEREFOR

EXPLANATORY NOTE

The rapid digitization of the Philippine financial ecosystem has greatly advanced financial inclusion, allowing millions of Filipinos to perform seamless banking, e-wallet transactions, instant credit line drawdowns, and digital loan applications directly through mobile devices. However, this shift has created a significant statutory gap that criminals actively exploit through mobile phone theft, robbery, SIM-swapping, and digital identity compromise.

When a mobile device is lost, stolen, or compromised, perpetrators nowadays can swiftly drain bank accounts, exhaust e-wallet balances, make unauthorized QR/merchant payments, and incur fraudulent digital loans or credit line drawdowns within minutes. Crucially, the current regulatory framework, including Republic Act No. 12010 (Anti-Financial Account Scamming Act or AFASA) and Bangko Sentral ng Pilipinas (BSP) Circular No. 1213, imposes obligations on individual institutions to provide 24/7 reporting channels and "Kill Switch" functionalities.¹ However, it lacks a unified, cross-institutional mechanism. A victim robbed of an unlocked phone containing multiple financial apps is currently forced to navigate fragmented reporting hotlines across dozens of individual institutions while the crime is actively occurring.

Furthermore, existing legal procedures often castigate victims by requiring a formal police report prior to emergency account suspension. In practice, obtaining a police report takes hours or days, by which time financial accounts are fully drained and fraudulent obligations incurred.

This bill seeks to address these vital gaps by establishing the 'Stolen Device Financial Protection Act.' The centerpiece of this measure is a statutory framework known as the National Financial Account Emergency Blocking System (NFAEBS).

¹ Bangko Sentral ng Pilipinas. (2025). *Anti-Financial Account Scamming Act (AFASA) booklet with IRRs* (Republic Act No. 12010). Bangko Sentral ng Pilipinas. <https://www.bsp.gov.ph/Regulations/Banking%20Laws/AFASA-Booklet-with-IRRs.pdf>

Through a single verified report made via any participating financial institution, centralized portal, hotline, public telecommunications entity, or law enforcement agency, an emergency notice immediately propagates across all covered financial institutions and telecommunications entities associated with the compromised mobile number, device (IMEI), or account credentials.

The bill seeks to establish a mechanism which will mandate immediate emergency blocking of high-risk transactions, and will provide for formal dispute resolution, police documentation, internal investigation, and permanent discharge of unauthorized obligations, to ensure maximum protection without procedural delays.

By closing operational gaps, integrating telecommunications providers alongside financial service providers, and creating a unified emergency defense system, this bill safeguards public trust in the digital economy and ensures that innocent victims do not bear the burden of criminal fraud.

In view of the foregoing, the immediate passage of this bill is earnestly sought.



Keith Micah "Atty. Mike" D.L. Tan
4th District, Quezon

Republic of the Philippines
HOUSE OF REPRESENTATIVES
Quezon City

TWENTIETH CONGRESS
Second Regular Session

HOUSE BILL NO. 11333

Introduced by: Hon. Keith Micah "Atty. Mike" D.L. Tan

AN ACT

ESTABLISHING AN EMERGENCY FINANCIAL ACCOUNT BLOCKING MECHANISM FOR LOST, STOLEN, OR COMPROMISED MOBILE DEVICES, PROTECTING CONSUMERS FROM UNAUTHORIZED DIGITAL FINANCIAL TRANSACTIONS, PRESCRIBING OBLIGATIONS OF FINANCIAL SERVICE PROVIDERS AND OTHER COVERED ENTITIES, AND PROVIDING PENALTIES THEREFOR

Be it enacted by the Senate and the House of Representatives of the Philippines in Congress assembled:

SECTION 1. *Short Title.* — This Act shall be known as the "Stolen Device Financial Protection Act."

SEC. 2. *Declaration of Policy.* — It is the policy of the State to protect consumers from deceptive, unfair, and unconscionable financial practices, and to ensure that digital financial innovations do not become instruments of economic victimization. In furtherance thereof, the State shall establish a prompt, unified, and cross-institutional emergency protection framework to safeguard financial accounts linked to lost, stolen, or compromised mobile devices, ensuring that victims are not held civilly, administratively, or financially liable for unauthorized transactions, credit line drawdowns, digital loans, or fund transfers executed through compromised credentials.

SEC. 3. *Definition of Terms.* — As used in this Act:

- (a) *Covered Financial Institution or Digital Financial Service Provider (DFSP)* refers to any bank, non-bank financial institution, electronic money issuer (EMI), virtual asset service provider, digital credit platform, financing company, or fintech entity offering mobile banking, e-wallet, instant credit lines, or digital loan services regulated by the Bangko Sentral ng Pilipinas (BSP) or the Securities and Exchange Commission (SEC);
- (b) *Covered Entity* includes DFSPs, Public Telecommunications Entities (PTEs), and registered digital payment system operators;
- (c) *Compromised Mobile Device or Account* refers to a mobile phone, SIM card, digital identity, or financial account credential that has been lost, stolen, forcibly taken, unlawfully accessed, intercepted, or subjected to unauthorized control or SIM-swapping;
- (d) *Emergency Notice* refers to an immediate notification transmitted by an account holder, authorized representative, or participating agency through any verified

channel reporting a lost, stolen, or compromised mobile device or financial account;

- (e) *Unauthorized Digital Transaction* refers to any fund transfer, withdrawal, digital loan application, credit line drawdown, merchant/QR payment, or credential modification executed on or after the estimated time of device loss or compromise without the genuine knowledge and consent of the account holder.

SEC. 4. *Right to Emergency Financial Account Protection*. — Every consumer shall have the statutory right to immediately request and receive emergency blocking of outgoing financial transactions and high-risk account modifications across all linked financial accounts upon reporting a lost, stolen, or compromised mobile device. Emergency blocking under this Section shall be executed immediately upon verification of the reporter's identity through alternative authentication methods and shall not require the prior presentation or filing of a police report, blotter, or formal affidavit.

SEC. 5. *National Financial Account Emergency Blocking System (NFAEBS)*. — There is hereby established the National Financial Account Emergency Blocking System (NFAEBS), a centralized, inter-operable real-time emergency reporting network managed jointly by the Department of Information and Communications Technology (DICT), the PNP Anti-Cybercrime Group (PNP-ACG), the National Bureau of Investigation (NBI), the BSP, and the National Telecommunications Commission (NTC).

The NFAEBS shall operate a 24/7 centralized hotline and digital portal enabling a single emergency report to trigger automated, simultaneous emergency blocking notices to all covered institutions linked to the reported mobile number, IMEI, or account identity.

SEC. 6. *Modes of Reporting and Identity Verification*. — An emergency report under this Act may be initiated through any of the following authorized channels: (a) any participating DFSP; (b) the centralized NFAEBS portal or hotline; (c) participating Public Telecommunications Entities (PTEs); or (d) designated law enforcement stations.

Covered entities shall establish flexible, multi-tiered identity verification mechanisms (including knowledge-based questions, alternate verified contacts, or remote biometric checks) to allow victims who have lost access to their primary mobile device and registered mobile number to rapidly authenticate their identity.

SEC. 7. *Immediate Duties of Covered Financial Institutions*. — Upon receipt of an Emergency Notice directly from the account holder or via the NFAEBS network, a covered DFSP shall, within a maximum response time to be prescribed by the BSP not exceeding fifteen (15) minutes, restrict and suspend the following outgoing and high-risk operations on all affected accounts:

- (a) Outgoing fund transfers, peer-to-peer payments, and cash withdrawals;
- (b) Digital loan applications, micro-loan approvals, and credit line drawdowns;
- (c) Merchant and QR code payments;
- (d) Changes to passwords, PINs, or security credentials;
- (e) Device or re-device enrollments;

- (f) Addition or modification of beneficiaries or linked bank accounts;
- (g) Changes to registered mobile numbers or email addresses; and
- (h) Account recovery requests initiated from the compromised device.

Provided, That incoming credits, salary deposits, legitimate remittances, and scheduled inward transactions shall remain permitted unless otherwise directed by the account holder or regulatory authority.

SEC. 8. *Coordination with Telecommunications Providers and NTC.* — Public Telecommunications Entities (PTEs) shall integrate their emergency SIM-suspension and device-blocking systems with the NFAEBS. Upon receipt of a verified report of a stolen or lost mobile device, PTEs shall immediately suspend SIM network connectivity and initiate International Mobile Equipment Identity (IMEI) blacklisting in coordination with the NTC, preventing unauthorized interception of One-Time Passwords (OTPs) and unauthorized network access.

SEC. 9. *Treatment of Pending and Subsequent Transactions.* — All outgoing transactions, credit line drawdowns, and digital loan disbursements initiated on or after the verified time of device loss, theft, or compromise shall be suspended immediately. Any pending transaction not fully settled prior to receipt of the Emergency Notice shall be cancelled without penalty to the consumer.

SEC. 10. *Disputed Transactions and Presumption of Unauthorized Use.* — Where a consumer submits a formal dispute accompanied by a sworn statement or an official PNP/NBI Incident Report certifying the loss, theft, or compromise of a mobile device within a reasonable period prescribed by IRR, any consumer-initiated transaction executed during or after the reported time of compromise requiring authentication or account access shall be presumptively considered unauthorized and fraudulent. *Provided*, That this presumption shall not automatically apply to previously authorized recurring transactions, standing debit instructions, or legitimate pre-scheduled payments.

SEC. 11. *Investigation and Burden of Proof.* — Upon receipt of a disputed transaction notice under Section 10, the covered DFSP shall conduct an expedited internal investigation completed within thirty (30) calendar days. The DFSP shall bear the legal burden of proving by substantial evidence that the disputed transaction was knowingly and voluntarily authorized by the account holder.

The mere showing that a transaction was completed using a correct One-Time Password (OTP), Mobile PIN (MPIN), or biometric match captured via the compromised device shall not alone be conclusive proof of consumer authorization or consent, where circumstantial or forensic evidence indicates the device was stolen or compromised.

SEC. 12. *Non-Liability and Permanent Discharge of Obligations.* — Upon confirmation through internal investigation or administrative determination that a disputed transaction or digital loan was unauthorized, the DFSP shall:

- (a) Permanently discharge and cancel the loan obligation, interest, and accrued penalties from the victim's name;

- (b) Fully credit back and restore any unauthorized fund transfer or balance deduction;
- (c) Refrain from reporting, and immediately reverse any adverse reporting of, the consumer to credit bureaus, credit information corporations, or collection agencies; and
- (d) Cease all collection activities against the victim.

It shall be unlawful for any DFSP, financing company, or collection agency to demand payment, harass, or initiate legal proceedings against a victim for a verified unauthorized transaction under this Act.

SEC. 13. *Restoration and Reactivation of Accounts.* — Covered DFSPs shall establish secure, standardized procedures for restoring account access and unfreezing legitimate funds once the consumer has secured a replacement device, new SIM card, or re-authenticated identity through verified in-person or enhanced digital verification methods.

SEC. 14. *Fraud Prevention and Authentication Standards.* — The BSP shall prescribe risk-based authentication and fraud-prevention standards for all DFSPs, including enhanced multi-factor authentication for high-risk transactions, dynamic behavioral monitoring, device fingerprinting, velocity tracking, and mandatory risk-based cooling-off periods following credential resets, device re-enrollments, or unusual loan requests.

SEC. 15. *Consumer Assistance and Appeals.* — Any consumer aggrieved by a DFSP's failure to apply emergency blocking, failure to conduct an expedited investigation, or improper denial of non-liability under this Act may lodge an administrative complaint with the BSP Consumer Assistance Mechanism or the SEC, without prejudice to judicial remedies under RA 11765 (Financial Products and Services Consumer Protection Act).

SEC. 16. *False or Fraudulent Reports.* — Any person who willfully files a false report of device theft, stages a simulated robbery, or fraudulently invokes the protections of this Act to evade legitimate monetary obligations shall be criminally liable under applicable provisions of the Revised Penal Code, including Article 183 (Perjury) and Article 315 (Estafa), and shall be liable for civil damages to affected covered entities.

SEC. 17. *Administrative Sanctions.* — Any covered entity that fails or refuses to comply with the emergency blocking, investigation, or obligation discharge mandates under this Act shall be subject to administrative fines ranging from One Hundred Thousand Pesos (PhP 100,000.00) to Five Million Pesos (PhP 5,000,000.00) per violation, alongside administrative sanctions, suspension of licenses, or enforcement actions imposed by the BSP, SEC, or NTC.

SEC. 18. *Penalties.* — Any representative, officer, or collection agent of a DFSP or third-party collection agency who knowingly enforces collection or engages in harassment for a verified unauthorized obligation covered under this Act shall suffer the penalty of imprisonment from six (6) months to two (2) years, or a fine ranging from Fifty Thousand Pesos (PhP 50,000.00) to Five Hundred Thousand Pesos (PhP 500,000.00), or both, at the discretion of the court.

SEC. 19. *Data Privacy and Information Sharing.* — The sharing of technical indicators, phone numbers, IMEIs, and transaction logs between covered entities, law enforcement, and the NFAEBS solely for emergency blocking and fraud investigation under this Act shall be recognized as lawful processing under Republic Act No. 10173 (Data Privacy Act of 2012), subject to strict data security and confidentiality protocols.

SEC. 20. *Implementing Rules and Regulations.* — Within ninety (90) days from the effectivity of this Act, the BSP, in consultation with DICT, PNP, NBI, NTC, SEC, National Privacy Commission (NPC), and representative fintech and banking associations, shall promulgate the necessary Implementing Rules and Regulations (IRR) for the effective execution of this Act.

SEC. 21. *Separability Clause.* — If any provision or part of this Act is declared unconstitutional or invalid, the remaining provisions not affected thereby shall continue to be in full force and effect.

SEC. 22. *Repealing Clause.* — All laws, executive orders, administrative orders, rules, and regulations inconsistent with or contrary to the provisions of this Act are hereby repealed, amended, or modified accordingly.

SEC. 23. *Effectivity.* — This Act shall take effect fifteen (15) days after its publication in the Official Gazette or in two (2) newspapers of general circulation in the Philippines.

Approved,