Crypto ATM Fraud Prevention Act—Section-by-Section Summary
Senator Dick Durbin (D-IL)

Section 1. Short Title.

This section specifies that the bill may be cited as the "Crypto ATM Fraud Prevention Act of 2025"

Section 2. Registration with the Secretary of the Treasury.

This section amends an existing provision of law, 31 U.S.C. § 5330, to require cryptocurrency ATM operators (referred to in this Act as "virtual currency kiosk operators") to register with the Secretary of the Treasury. These operators currently are required to register pursuant to Treasury regulations that define them as "money transmitting businesses." This provision merely codifies that requirement into statute.

This section also requires virtual currency kiosk operators to disclose the physical locations of all kiosks they own or operate to the Treasury Department, and to provide updates every 90 days.

Section 3. Prevention Fraudulent Transactions at Virtual Currency Kiosks

This section amends the Bank Secrecy Act (31 U.S.C. §§ 5311-36) by adding a new section (31 U.S.C. § 5337).

Definitions

This subsection establishes definitions for terms that are used throughout the bill. Notably, the Act defines a "Virtual Currency Kiosk" as "a stand-alone machine that is capable of accepting or dispensing legal tender in exchange for virtual currency." "Virtual currency kiosk operator" is defined as "a person who owns, operates, or manages a virtual kiosk located in the United States or its territories."

This subsection also establishes a definition of "new customer[s]," who are afforded a special level of protection by various provisions of the bill. A "new customer" is defined as "a customer during the 14-day period beginning on the date of the first virtual currency kiosk transaction of the customer with the virtual currency kiosk operator."

Disclosures

This subsection requires that virtual currency kiosk operators clearly disclose all relevant terms and conditions of each transaction to the customer and display a warning about the risk of fraud. The warning also must include warnings about the most common types of fraudulent scams involving cryptocurrency ATMs. Both disclosures must be made clearly and conspicuously before each transaction, and in an easily readable manner, and the operator must ensure that each customer acknowledges each disclosure.

Receipts

This subsection requires that operators issue receipts to customers after each transaction. Each receipt must include information sufficient to identify and trace the transaction, including the names of the kiosk operator and customer; the time, date, place, and amount of the transaction; amount of fees charged; and a transaction "hash" (a unique identifier). Receipts also must include information helpful to customers who may have been scammed, such as a phone number for a customer service helpline, a URL link to the operator's refund policy, and a statement that customers may be entitled to a refund for fraudulent activity within 30 days. The subsection also requires that operators begin issuing paper receipts to all customers within a year of the effective date of the Act (in practice, 15 months from enactment).

Anti-Fraud Policy

This subsection requires kiosk operators to develop a comprehensive anti-fraud policy, and to submit a copy of the policy to the Financial Crimes Enforcement Network at the Treasury Department. The purpose of this provision is to ensure that operators are thinking seriously about the risk of fraud at their kiosks, and to encourage them to develop specific steps and safeguards to reduce the incidence of fraud—while still giving operators flexibility to develop an anti-fraud strategy that works on their platform.

Compliance Officer

This subsection requires all kiosk operators to appoint a Chief Compliance Officer. This officer must not concurrently be the CEO, must be a full-time employee, and must not own more than twenty percent of the company. This ensures that the officer has sufficient bandwidth to devote to compliance responsibilities and minimizes conflicts of interest.

Blockchain Analytics

This subsection requires that operators use blockchain analytics tools to analyze and trace transactions, and to identify suspicious or fraudulent activity. Blockchain analytics are important tools for identifying fraudulent cryptocurrency transactions because traditional forensic tools are ineffective due to the anonymity of the blockchain.

Verbal Confirmation

This subsection requires that operators obtain live, verbal confirmation from new customers before proceeding with a transaction greater than $500. New customers are the most likely to be victims of fraud, and scammers will often try to keep in constant contact with their victims until the transaction is complete. This requirement is a way to break that contact and give the victim a chance to think clearly before making a payment. Also, this requirement forces operators to make an effort to determine whether a customer may be involved in a scam.

Refunds

This subsection allows customers who were victims of fraud to get a refund, subject to certain requirements. To get a refund, the customer will have to make a report to a law enforcement agency—including a sworn affidavit—and a report to the kiosk operator, both within 30 days of the transaction. This dual reporting requirement reduces the risk that customers will lie to get a refund.

New customers are entitled to a full refund, and other customers are entitled to have their fees refunded. Because these kiosks often charge fees as high as 20-30% of the value of the transaction, these fees can be significant. Finally, this subsection entitles customers to damages in the case that they are denied a refund in violation of this subsection. This is to ensure that operators readily comply with this provision.

Transaction Limits

This subsection establishes limits on the amount of money a kiosk operator can accept from a new customer (that is, during a customer's first 14 days). New customers would be prevented from depositing more than $2,000 per day with a kiosk operator, and $10,000 over the first 14 days. This is meant to limit the amount that a potential fraud victim can lose to scammers before they have the chance to realize that they are being scammed.

Customer Service Helpline

This subsection requires operators to provide a live customer service helpline that is available during all hours that the operator accepts transactions. The helpline would have to be regularly monitored.

Communications with Law Enforcement

This subsection requires operators to open a dedicated communications line through which law enforcement can contact the operator about suspected fraudulent activity. The communications line would have to be an email or phone number that is regularly monitored and must be communicated to relevant law enforcement within 90 days of the effective date.

Civil Penalties

This subsection creates civil penalties to ensure compliance with the provisions of the Act. Any violation would be subject to a $10,000 penalty, which would multiply each day the violation continues. This is to ensure that it is never economically efficient to violate the law. These penalties would be enforced by the Treasury Department.

Relationship to State Laws

This subsection merely clarifies that the Act does not preempt states from enacting laws or regulations that go further to protect consumers—for example, by establishing lower daily transaction limits. State laws would be preempted only if they directly conflict with the Act, or if they are more permissive.

Section 4. Effective Date

This section provides that the provisions of the Act shall take effect 90 days after the date of enactment. Note that some provisions of the Act take effect at certain times measured from the effective date. So, for instance, a provision scheduled to take effect 90 days after the effective date would actually take effect 180 days after enactment.