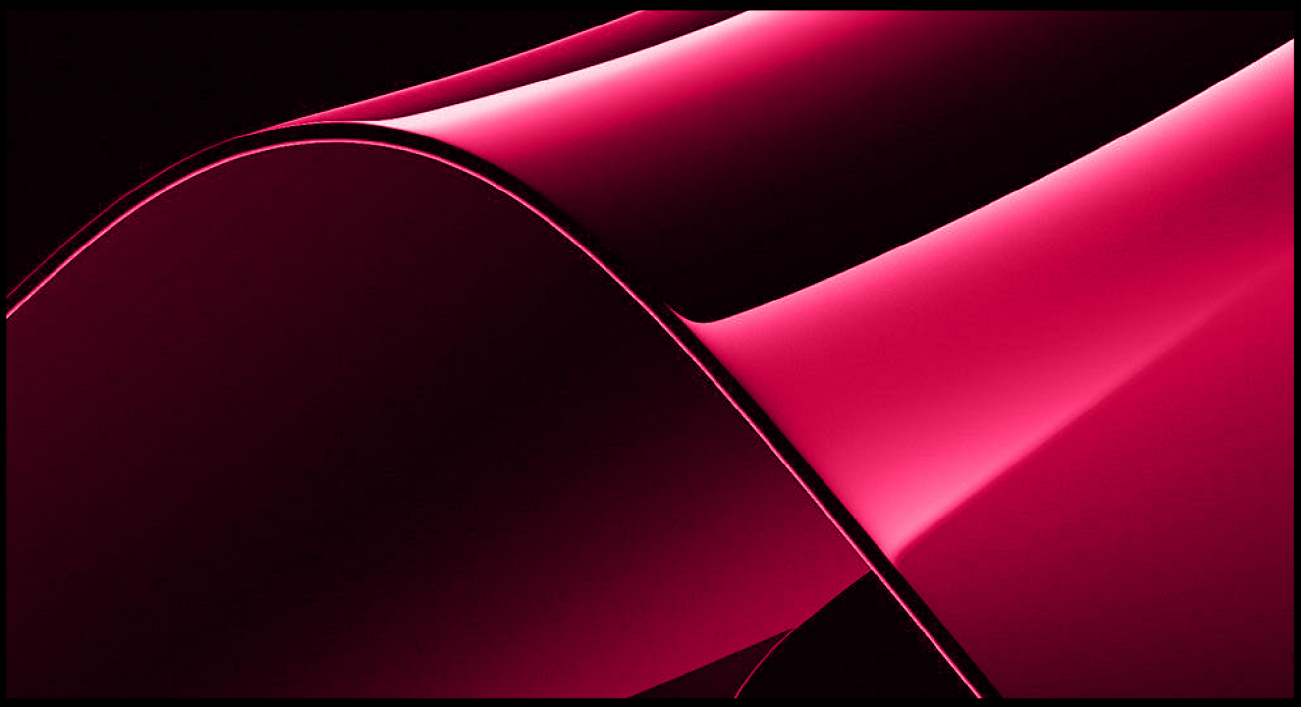
CERTIK
SKYNET

SKYNET
Crypto ATM Fraud Report

Crypto ATM fraud is one of the fastest-growing financial crime categories in the United States. Criminal organizations exploit the speed and pseudonymity of crypto kiosks to extract funds from vulnerable populations at an accelerating pace.



1. Executive Summary

Crypto ATM fraud is one of the fastest-growing financial crime categories in the United States. Criminal organizations exploit the speed and pseudonymity of crypto kiosks to extract funds from vulnerable populations at an accelerating pace.

Key Takeaways:

1. **Losses at crypto ATMs surged to $333.5 million in 2025, driven by the machines' speed and irreversibility.**
   The FBI recorded over 12,000 complaints between January and November 2025, a 33 percent increase over the prior year. The United States hosts 78 percent of the world's 45,000 crypto ATMs, and the machines' ability to convert cash to crypto in under five minutes with minimal identity verification makes them the lowest-friction extraction channel available to scammers.

2. **Crypto ATMs function as frontend terminals, not standalone devices, and this architecture creates a critical forensic gap.**
   Each kiosk routes transactions through a backend Crypto Application Server (CAS) that releases funds from the operator's commingled hot wallet. The public blockchain records only the operator-to-destination transfer, not the victim's identity. This Attribution Gap means law enforcement must subpoena operator CAS logs to link a physical cash deposit to an on-chain transaction, and the only effective technical intervention is real-time wallet screening at the CAS before the transaction is broadcast.

3. **Older adults account for 86 percent of losses, and existing kiosk-level safeguards are failing.**
   The D.C. Attorney General's case against Athena Bitcoin found that 93 percent of deposits on the company's machines were tied to fraud, with a median victim age of 71. On-screen warnings proved ineffective when victims were simultaneously being coached by a scammer on a live call. The case signals that operator awareness of fraud without adequate remediation may trigger enforcement under consumer protection and elder abuse statutes.

4. **Transnational criminal organizations are industrializing ATM-based extraction at unprecedented scale.**
   Attackers operate structured organizations with specialized divisions for lead generation, social engineering, and post-transaction laundering. Asian money laundering networks processed an estimated $16.1 billion in illicit crypto flows in 2025, clearing transactions in under two minutes through Telegram-coordinated services based in Southeast Asia.

5. **AI-augmented deepfakes and distributed low-value transaction models will erode current defenses.**
   AI-enabled scams were 4.5 times more profitable than traditional methods in 2025. As states implement transaction caps, criminal networks are pivoting to coordinated low-value deposits across dispersed kiosks, staying below regulatory thresholds while maintaining aggregate volume. The legislative response, with at least 14 states enacting or proposing crypto ATM-specific rules, remains fragmented.



2. Overview

2.1 Definition of Crypto ATM Fraud

Crypto ATM fraud is a form of financial exploitation in which criminals use social engineering to direct victims to cryptocurrency kiosks, where the victims withdraw and deposit physical cash that is immediately converted into digital assets and transmitted to wallet addresses controlled by the attackers. These kiosks are typically located in gas stations, convenience stores, and other retail environments. The fraud represents a direct evolution of earlier wire transfer and gift card scam methodologies, adapted to exploit the speed, irreversibility, and pseudonymity of blockchain-based transactions.

The process differs fundamentally from traditional banking fraud. Rather than compromising a victim's account credentials or intercepting digital transfers, the attacker manipulates the victim into voluntarily withdrawing cash from their own bank account and physically depositing it into a kiosk. The kiosk then converts the cash into cryptocurrency, typically Bitcoin, and routes it to a wallet address encoded in a QR code provided by the scammer. Once the transaction is broadcast to the blockchain, the funds are effectively removed from the regulated banking system. The victim cannot initiate a chargeback, and law enforcement faces significant barriers to recovery.

2.2 Historical Evolution

The migration toward crypto ATMs as a preferred fraud vector reflects a broader pattern of criminal adaptation to institutional countermeasures. In the early 2000s, social engineering scams relied primarily on wire transfer services such as Western Union, which carried relatively high interception risk and were subject to increasing institutional scrutiny. Criminals subsequently shifted to gift card-based extraction, instructing victims to purchase prepaid cards at retail locations and share the redemption codes by phone. As retailers implemented staff training programs to identify suspicious bulk purchases and as card issuers improved their fraud detection capabilities, this method also became less reliable.

The rapid proliferation of crypto ATMs beginning in the mid-2010s provided what criminal organizations recognized as a superior extraction mechanism. The global crypto ATM fleet grew from a few hundred machines in 2016 to approximately 40,000 by early 2024 and has since expanded to an estimated 45,000 units. These machines combine the accessibility of physical cash with the speed and pseudonymity of blockchain transactions, enabling criminals to move funds across international borders within minutes of the initial deposit. This has effectively transformed traditional impersonation scripts, such as the grandparent scam and government agency impersonation, into components of sophisticated, technology-enabled extraction operations.

Year	Reported Losses (USD)	Complaints (FBI IC3)	Primary Scam Type
2022	$78 million	Not disclosed	Lottery and Sweepstakes
2023	$114 million	Not disclosed	Government Impersonation
2024	$250 million	Not disclosed	Tech Support / Bank Fraud
2025 (Jan-Nov)	$333.5 million	12,000+	Multi-step Relationship Fraud

Figure 1: Escalation of Reported Crypto ATM Fraud Losses

2.3 Differentiation from Other Crypto Fraud Schemes

Crypto ATM fraud is distinguished from other digital asset crimes by its reliance on physical cash and its hybrid nature, bridging traditional banking infrastructure with blockchain networks. Unlike phishing or wallet-draining attacks, which require compromising private keys or tricking users into signing malicious smart contracts, ATM-based fraud relies entirely on social engineering to induce the victim to perform a voluntary physical action at a kiosk.

Exchange-based scams and fraudulent token offerings often involve the construction of elaborate fake investment platforms designed to sustain victim engagement over weeks or months. Crypto ATM fraud, by contrast, is optimized for high-velocity extraction. The machines allow near-instantaneous conversion of cash to cryptocurrency, bypassing the more rigorous know-your-customer protocols and cooling-off periods that characterize major centralized exchanges. This creates a structural vulnerability: while a bank might flag a suspicious wire transfer, it is far less likely to intervene when a customer withdraws cash in person, and once that cash enters the kiosk, the banking system's protective mechanisms no longer apply.

3. Categories and Classification

3.1 Types of Crypto ATM Fraud Attacks

Crypto ATM fraud schemes can be classified by the psychological mechanism used to drive the victim toward the kiosk. While the specific narratives vary, all approaches share a common structural objective: inducing a state of heightened emotional arousal that suppresses the victim's capacity for rational evaluation, isolating the victim from potential interveners, and guiding them through the cash-to-crypto conversion process in real time.

Approach	Psychological Mechanism	Manufactured Crisis	Typical Victim Profile	Average Loss
Law Enforcement Impersonation	Fear and urgency	Threat of arrest or asset seizure	Seniors, immigrants, individuals with limited legal knowledge	$8,000 - $15,000
Tech Support	Panic and confusion	Impending loss of banking access or personal data	Older adults with limited technical literacy	$5,000 - $12,000
Romance / Relationship Fraud	Trust and financial aspiration	Promise of relationship or financial independence	Socially isolated individuals across age groups	$10,000 - $50,000+
Grandparent Scam	Empathy and panic	Family member in immediate danger or legal trouble	Elderly adults with grandchildren	$5,000 - $20,000
Fraud Recovery	Hope and desperation	Claim of ability to recover previously lost funds	Prior scam victims across demographics	$3,000 - $10,000

Figure 2: Classification of Crypto ATM Fraud Approaches

Authority-based impersonation remains the most prevalent approach. Scammers pose as agents from the IRS, FBI, Social Security Administration, or local law enforcement, manufacturing a crisis involving a compromised Social Security number, a frozen bank account, or pending criminal charges. The victim is told that the only way to protect their assets is to move them into a government-certified digital account at a local kiosk. The effectiveness of this approach relies on the victim's unfamiliarity with cryptocurrency infrastructure and their assumption that a physical machine in a retail setting operates under the same consumer protections as a bank ATM.

Relationship-based fraud, commonly referred to as pig butchering, follows a longer timeline. The attacker builds trust through sustained communication over weeks or months, eventually introducing the crypto ATM as a vehicle for small initial deposits into a purported investment platform. The platform displays fabricated returns to encourage increasingly larger deposits. This approach accounted for the highest individual loss amounts in 2025 and has shown significant overlap with Southeast Asian scam compound operations.

An emerging data category identified in 2025 is fraud recovery targeting, in which individuals who have already lost money to an earlier scam are contacted by the same or affiliated criminal networks, which claim to be able to recover the lost funds for an upfront fee payable through a crypto ATM.

3.2 Classification of Targets

The victimology of crypto ATM fraud is heavily concentrated among older adults. An AARP analysis published in 2025 found that approximately 86 percent of all recorded losses involved victims over the age of 60. The D.C. Attorney General's investigation of Athena Bitcoin's operations found a median victim age of 71 across transactions processed on the company's machines in the District.

Several factors account for this concentration. Older adults are more likely to maintain significant liquid savings in accessible accounts. Research indicates a measurable digital literacy gap regarding the distinction between traditional bank ATMs and cryptocurrency kiosks, with many seniors assuming that a physical machine in a familiar retail environment offers the same reversible protections as a bank-affiliated terminal. Social isolation further compounds vulnerability, particularly when scammers deploy AI-generated voice cloning or deepfake video technology to mimic the voices or appearances of trusted family members or known local officials.

The FBI's IC3 data from 2025 also reveals an important secondary demographic trend: victims under 40 are increasingly appearing in relationship fraud and fake investment scheme complaints, though their per-incident losses tend to be lower than those of older victims.

3.3 Fraud Access Vector

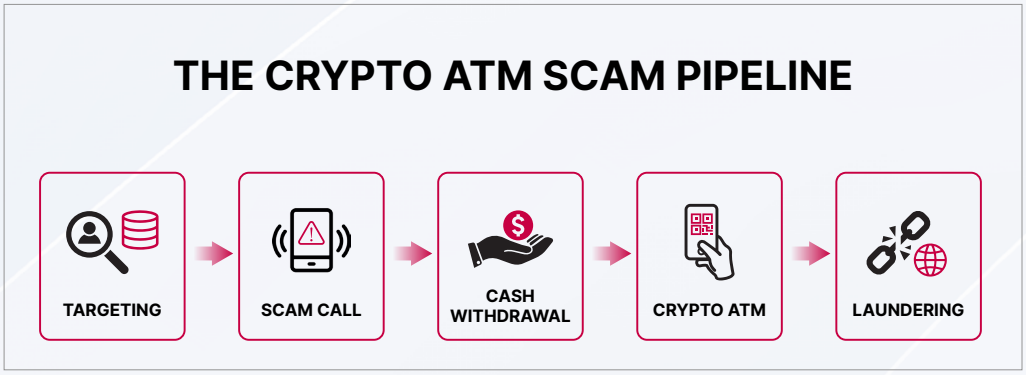


Figure 3: Crypto ATM Scam Pipeline

The attack pipeline begins well before the victim reaches a kiosk. Initial targeting typically originates from large-scale data breaches and illicit data brokerages that compile and sell curated lists of vulnerable individuals to criminal organizations. These lists often include demographic indicators such as age, geographic location, financial institution affiliation, and prior scam exposure, enabling highly targeted outreach.

Criminal networks use these lead lists to launch automated smishing (SMS phishing) and vishing (voice phishing) campaigns. The initial contact is designed to induce heightened emotional arousal, whether through fear of arrest, excitement over a romantic connection, or panic over a family member's safety. Once the target engages, the attacker transitions into a sustained coaching role, maintaining a continuous phone or video connection to isolate the victim from potential intervention by family members, bank employees, or bystanders.

By the time the victim arrives at the kiosk, they have typically been conditioned over the course of 30 minutes to several hours to view the machine as a necessary tool for protecting their assets or helping a loved one. The attacker provides real-time guidance through the transaction process, including instructions on how to respond to any on-screen fraud warnings and what to tell bank tellers if questioned about the cash withdrawal.

3.4 Technical Architecture and Attribution Challenges

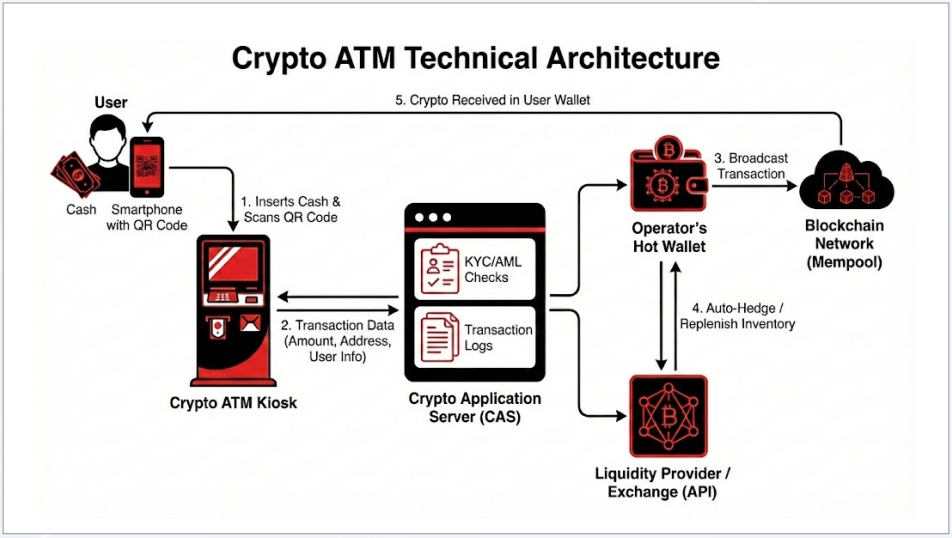


Figure 4: Crypto ATM Technical Architecture Diagram

Understanding the technical infrastructure of crypto ATMs is essential for evaluating both the persistence of this fraud vector and the available intervention points. Contrary to the common perception that crypto ATMs function as standalone vending machines containing digital assets, they operate primarily as frontend terminals connected to a backend Crypto Application Server, or CAS. When a user inserts cash and scans a QR code, the kiosk does not transmit a transaction directly to the blockchain. Instead, it signals the CAS to release funds from the operator's centralized hot wallet to the destination address. The system simultaneously triggers an automated API call to a liquidity provider or exchange, such as Kraken or Coinbase, to hedge against price volatility and replenish the operator's cryptocurrency inventory.

This architecture creates a significant forensic challenge. Because on-chain transactions originate from the operator's commingled hot wallet rather than from a user-specific address, the public blockchain ledger records only a transfer from the operator to the destination wallet. The critical link between the victim's identity and the recipient address exists only within the operator's internal CAS logs. Law enforcement cannot reconstruct this link from the blockchain alone; they must subpoena operator records to bridge the gap between the physical cash deposit and the on-chain transaction. This problem is referred to in this report as the Attribution Gap.

Tiered Verification Exploitation

Most modern crypto ATMs implement tiered identity verification proportional to transaction size. At the lowest tier, typically covering transactions below $500 to $1,000, the machine requires only SMS or phone-based verification. Higher-value transactions trigger requirements for government-issued identification, biometric scans, or Social Security number validation. Criminal organizations have adapted to these thresholds by coaching victims to structure their deposits, keeping individual transactions within lower verification tiers to avoid triggering enhanced identity checks. This structuring behavior is itself a federal crime under the Bank Secrecy Act, though enforcement in the crypto ATM context has been limited.

The Ingress Point as the Critical Intervention Window

Once funds leave the operator's hot wallet and settle on the blockchain, the laundering process merges with generic on-chain obfuscation flows, including mixing services, cross-chain bridge protocols, and decentralized exchange routing. At that point, the laundering activity is no longer specific to the ATM fraud vector and becomes indistinguishable from other illicit fund flows. The only technically unique variable in the crypto ATM fraud pipeline, and therefore the most effective point of intervention, is the ingress point at the CAS level. Effective mitigation requires real-time screening of destination wallet addresses against known blocklists before the CAS broadcasts the transaction to the blockchain mempool.

4. 2025 Threat Landscape

4.1 Global Statistics

The scale of crypto ATM fraud reached unprecedented levels in 2025. Between January and November, the FBI's IC3 recorded more than 12,000 complaints and $333.5 million in cumulative losses, representing a 33 percent increase over the $250 million reported during the comparable period in 2024. The losses through the first half of 2025 alone reached $240 million, roughly double the pace of the prior year. The FBI characterized the trajectory as showing a clear and constant rise that is not slowing down.

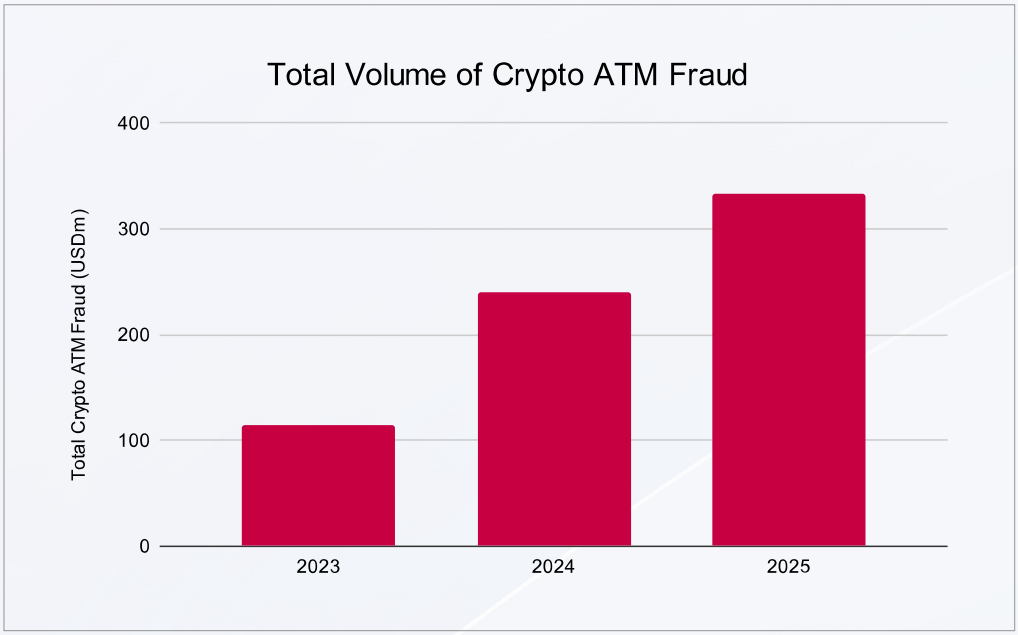


Figure 5: Total Volume of Crypto ATM Fraud

The global crypto ATM market is heavily concentrated in North America. The United States hosts approximately 78 percent of the world's 45,000 crypto ATMs, followed by Canada at 9.4 percent, Australia at 5.2 percent, and the remainder distributed across Europe, Asia, and Latin America. Within the United States, Florida, California, and Texas consistently report the highest loss volumes, driven by the high density of kiosks in urban retail environments.

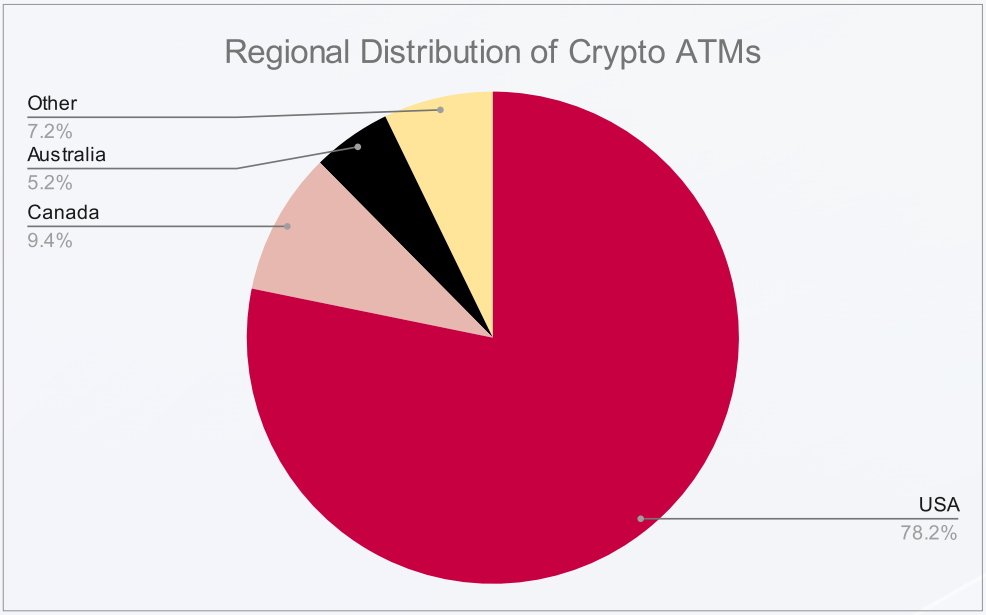


Figure 6: Regional Distribution of Crypto ATMs

The broader crypto fraud ecosystem provides important context for these figures. Chainalysis estimated in its 2026 Crypto Crime Report that at least $14 billion was received on-chain by scam operations in 2025, with impersonation scams showing a reported 1,400 percent year-over-year increase. AI-enabled scams were found to be 4.5 times more profitable than traditional scam methods, reflecting the rapidly increasing sophistication of social engineering infrastructure.

4.2 Key Enforcement Actions

A landmark enforcement action in 2025 was the lawsuit filed by the D.C. Attorney General against Athena Bitcoin, Inc., one of the largest crypto ATM operators in the United States, which operates approximately 4,100 machines across five countries. The complaint, filed in September 2025, alleged that 93 percent of all deposits made through Athena's seven kiosks in the District of Columbia were linked to fraud. The investigation found a median victim age of 71 and median per-transaction losses of $8,000.

The D.C. Attorney General's complaint further alleged that Athena imposed undisclosed transaction markups of 13 to 26 percent, significantly exceeding the 0.24 to 3 percent fees typical of major cryptocurrency exchanges. These fees were embedded within the displayed exchange rate and never separately disclosed to the consumer. When scam victims sought refunds, Athena enforced a strict no-refund policy and in some cases required victims to sign releases absolving the company of future liability. The company's own internal logs showed that 48 percent of all deposits during its first five months of operation in the District resulted in the customer reporting directly to Athena that they had been scammed.

In August 2025, FinCEN issued a formal alert reminding financial institutions that crypto ATM operators are classified as money services businesses under the Bank Secrecy Act, with corresponding obligations for registration, anti-money-laundering programs, and suspicious activity reporting. The alert specifically highlighted the use of these machines in tech-support and bank-impersonation scams targeting older adults.

4.3 Regional Distribution and Laundering Networks

While the physical extraction of funds occurs overwhelmingly at kiosks in Western nations, the financial infrastructure used to process and obscure stolen funds is anchored in jurisdictions with limited regulatory oversight. There are reports that Asian-language money laundering networks processed an estimated $16.1 billion in illicit cryptocurrency flows in 2025, equivalent to approximately $44 million per day. These networks accounted for roughly 20 percent of the attributed global illicit crypto ecosystem and have grown at a rate more than 7,000 times faster than flows to centralized exchanges since 2020.

These laundering operations are primarily coordinated through Telegram-based channels that function as marketplace hubs, connecting criminal clients with launderers who advertise their services alongside proof-of-liquidity imagery. The operational hubs for these networks are concentrated in Southeast Asia, particularly within the tri-border region of Myanmar, Laos, and Thailand, as well as Cambodia. The United Nations Office on Drugs and Crime has estimated that countries in East and Southeast Asia lost approximately $37 billion to cybercrime in 2025, with scam compound revenue representing a significant share of GDP in certain jurisdictions.

This geographic structure creates a stark enforcement asymmetry: victims are located in Western nations with high kiosk accessibility, while the laundering infrastructure operates from jurisdictions with minimal regulatory reach, making cross-border recovery extremely difficult.

5. Attacker Profiles

5.1 Profile of Attackers

The profile of crypto ATM fraud operators has shifted decisively from independent actors to structured transnational criminal organizations that operate with corporate-level division of labor. These organizations are concentrated in jurisdictional safe havens across Southeast Asia, particularly the tri-border region of Myanmar, Laos, and Thailand, and in parts of Eastern Europe. Operations are often conducted from fortified compound facilities that house hundreds of workers.

The organizational structure typically includes specialized divisions for each phase of the fraud pipeline: lead generation and data harvesting teams that acquire and curate victim lists; psychological specialists trained as closers who conduct the phone-based social engineering; and money movement teams consisting of mules and launderers who manage the digital transfer and obfuscation of funds after the ATM transaction. Frontline phone operators are in many cases themselves victims of human trafficking, recruited through fraudulent job advertisements and coerced into conducting scams from compound facilities. There are reports that cryptocurrency flows to suspected human trafficking services associated with these operations surged 85 percent in 2025.

The organizations are well-capitalized, investing in advanced AI voice-cloning technology, deepfake video generation tools, and operational security infrastructure. This produces a characteristic split profile: the backend technology and laundering operations are highly sophisticated and automated, while the customer-facing element is a patient, empathetic human actor specifically trained to exploit the cultural and emotional vulnerabilities of Western victims.

5.2 Tactics and Procedures

The procedural framework governing crypto ATM fraud is built around maintaining continuous control over the victim throughout the extraction process. Initial contact is typically automated and multichannel, with victims receiving coordinated SMS messages, emails, and phone calls that appear to originate from trusted institutions through caller ID spoofing and domain mimicry.

Once a victim engages, the attacker initiates a sustained live connection, often referred to operationally as a stay-on-the-line protocol. This continuous phone presence serves a critical tactical function: by keeping the victim on the call through the bank withdrawal, the drive to the kiosk, and the deposit process, the attacker prevents the victim from consulting family members, bank tellers, or law enforcement who might recognize the fraud in progress.

Attackers also provide victims with scripted cover stories for bank interactions, instructing them to tell tellers that the cash withdrawal is for a home renovation, vehicle purchase, or family emergency. These cover stories are specifically designed to avoid triggering anti-money-laundering alerts that might otherwise prompt bank staff to intervene.

5.3 Social Engineering

The social engineering methodology centers on inducing and sustaining a state of cognitive overload that impairs the victim's ability to evaluate the situation rationally. Attackers are trained to oscillate between aggressive pressure and protective empathy depending on the fraud approach. In authority impersonation schemes, this manifests as threats of immediate arrest paired with assurances that the attacker is the only person who can help secure the victim's assets. In relationship fraud, the emotional manipulation builds gradually over weeks or months before the financial extraction begins.

A technique that became increasingly common in 2025 is authority nesting, in which the primary caller hands the phone to a supposed supervisor, federal agent, or department head to reinforce the illusion of a legitimate institutional process. The attackers also deploy compelled secrecy directives, telling victims that because of a gag order, an active investigation, or a security breach at their bank, they must not disclose the transaction to anyone. This effectively isolates the victim within a manufactured informational environment controlled entirely by the attacker.

5.4 Technology and Operational Security

Criminal organizations engaged in crypto ATM fraud deploy a sophisticated technology stack to maintain anonymity and ensure the finality of each theft. Key elements include virtual private servers and VPN infrastructure that mask the geographic origin of calls, making contacts from Southeast Asian compound facilities appear as calls from local U.S. area codes. QR codes encoding destination wallet addresses are often generated dynamically and set to expire shortly after a single use, reducing the window available for forensic analysis.

On the post-transaction side, automated laundering protocols route funds through chain-hopping services, decentralized mixing protocols, or cross-chain bridge infrastructure within minutes of transaction confirmation. In many cases, the funds have passed through multiple obfuscation layers before the victim has ended the phone call. The emergence of Asian-language money laundering networks that can clear large transactions in under two minutes has further compressed the window available for intervention.

6. Detection and Mitigation Strategies

6.1 Technical Detection and Mitigation

Technical countermeasures operate across three layers: on-chain analytics, kiosk-level behavioral monitoring, and network-level intelligence sharing.

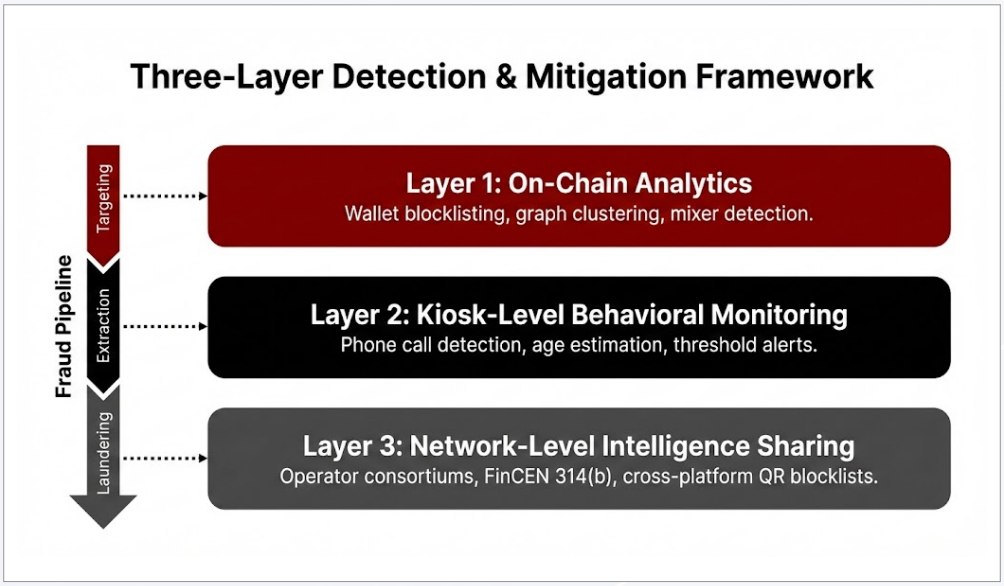


Figure 7: Three Layer Defense Framework

On-chain analytics platforms continuously monitor blockchain transactions for patterns indicative of fraud. These systems identify wallets that receive funds from kiosk transactions and immediately route them through known mixing services, tumbler contracts, or cross-chain bridges. When a flagged wallet is detected, operators can be alerted in real time to halt pending transactions or blocklist the associated QR code. Advanced implementations use graph-based clustering algorithms to link apparently unrelated wallets to the same criminal entity, enabling preemptive blocklisting before a wallet is used in a new fraud event.

At the kiosk level, behavioral analytics systems are being deployed to detect anomalous patterns during the transaction process. These systems monitor for indicators such as first-time users attempting transactions near maximum thresholds, repeated transactions from the same user within short intervals, and users who appear to be on active phone calls while operating the machine. Some operators have begun testing camera-based age estimation to flag transactions initiated by elderly users for additional verification, though privacy considerations have limited broad deployment.

Network-level intelligence sharing has advanced significantly. In 2025, major operators including Bitcoin Depot, CoinFlip, and Coinme established a voluntary consortium to share blocklisted wallet addresses and known scam QR codes across their combined networks, reducing the time between initial fraud detection at one operator and industry-wide blocking from days to hours. FinCEN's 314(b) program continues to provide a regulatory framework for information sharing between kiosk operators and law enforcement.

An emerging technical approach involves the deployment of risk-calibrated delay systems that impose algorithmically determined hold periods on transactions flagged as high-risk. Unlike blanket cooling-off periods, these systems use machine learning models trained on historical fraud data to assess individual transaction risk in real time, applying holds only when the estimated fraud probability exceeds a calibrated threshold. This approach seeks to balance consumer convenience with fraud prevention while minimizing false positives that could discourage legitimate kiosk usage.

6.2 Consumer Awareness

Public awareness remains the single most effective upstream intervention against crypto ATM fraud, as the vast majority of these schemes depend entirely on the victim's lack of knowledge about how cryptocurrency transactions function and what protections they do and do not offer.

The year 2025 saw a marked increase in awareness campaigns. AARP expanded its fraud prevention programming with targeted outreach to older adults about the specific risks of crypto ATMs. State and local law enforcement agencies across more than 20 states issued public advisories. The Arizona Attorney General published a crypto ATM fraud alert in February 2026. The California Department of Financial Protection and Innovation issued a formal consumer protection framework stating that no legitimate organization will ever ask a consumer to deposit cash into a crypto ATM to resolve an issue or protect their money.

At the kiosk level, several states now require operators to display un-skippable, high-contrast warning screens describing common fraud scenarios before any transaction can proceed. Florida's SB 505, effective in 2026, mandates specific warning language and requires operators to maintain 24/7 fraud reporting hotlines. However, the D.C. Attorney General's investigation of Athena Bitcoin found that on-screen warnings were largely ineffective when victims were simultaneously being coached through the process by a scammer on a live phone call.

6.3 Legislative Measures

The legislative response to crypto ATM fraud has accelerated across multiple jurisdictions, though implementation remains uneven.

European Union

The EU's Markets in Crypto-Assets Regulation, known as MiCA, entered full application in December 2024 and establishes a comprehensive framework directly affecting crypto ATM operations within EU member states. Under MiCA, any entity facilitating the exchange of fiat currency to crypto-assets, including kiosk operators, must obtain authorization as a Crypto-Asset Service Provider. This authorization carries mandatory KYC verification, transaction monitoring obligations, and suspicious transaction reporting requirements. MiCA's travel rule provisions require that originator and beneficiary information accompany crypto transfers, significantly reducing the anonymity that makes ATM-based fraud viable. The compliance burden has led several operators to voluntarily exit the EU market.

United States Federal

The Crypto ATM Fraud Prevention Act of 2025, introduced in the U.S. Senate in February 2025, would mandate a 14-day new-user onboarding period with a maximum daily transaction limit of $2,000 and a cumulative cap of $10,000 during that period. The bill also requires verbal confirmation for transactions exceeding $500 and un-skippable warning screens. As of early 2026, the bill has been referred to the Senate Banking Committee but has not advanced to a vote.

U.S. State-Level Legislation

State legislatures have moved more aggressively than the federal government. At least 14 states enacted or proposed crypto ATM-specific legislation in 2025 and early 2026. California's Digital Financial Asset Law, effective since January 2024, imposes a $1,000 daily transaction limit per individual and requires biometric identity verification for transactions exceeding $500. Florida's SB 505 mandates un-skippable warning screens and operator-maintained fraud reporting hotlines. Vermont and Connecticut have pursued moratoriums on new kiosk installations pending the development of comprehensive regulatory frameworks. Indiana's legislature advanced HB 1116, which would prohibit crypto ATM operations within the state entirely. Today, the regulatory landscape across states remains largely fragmented, with only a small number of states enacting restrictive legislation.

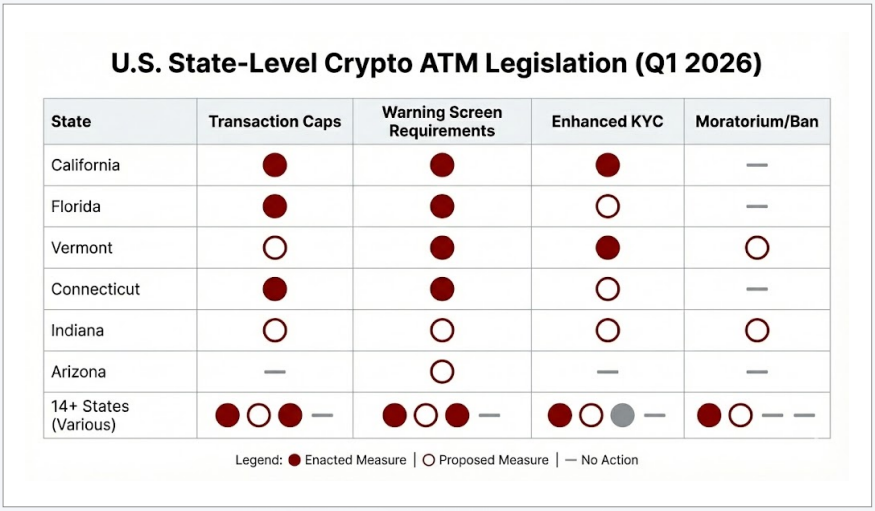


Figure 8: U.S. State-Level Crypto ATM Legislation

In Australia, legislators have introduced measures to set daily transaction limits and restrict the further proliferation of crypto ATMs. Several U.S. municipalities, including Chico, California, have enacted local moratoriums on new kiosk permits.

7. Expected Threat Evolution

The trajectory of crypto ATM fraud points toward increasing automation, sophistication, and resilience against current countermeasures. Several trends are expected to define the threat landscape through 2026 and beyond.

AI-Augmented Social Engineering

The integration of real-time deepfake synthetic media into fraud operations represents the most significant near-term escalation. Attackers are moving beyond voice impersonation to deploy live face-swap technology for video calls, allowing them to visually impersonate trusted family members, local officials, or bank managers. AI-driven personalization tools enable scammers to scrape social media data and construct hyper-targeted scripts that mirror the specific language, appearance, and communication patterns of the victim's trusted contacts. It is reported that AI-enabled scams were 4.5 times more profitable than traditional methods in 2025, and the rapid improvement of commercially available deepfake tools suggests this multiplier will increase.

Automated Obfuscation Through DeFi and Cross-Chain Infrastructure

On the technical backend, criminal organizations are migrating away from static wallet addresses toward dynamically generated, single-use QR codes linked to decentralized liquidity pools or automated smart contract routing. This approach ensures that funds are immediately dispersed across multiple blockchains or converted into privacy-focused tokens upon receipt, rendering traditional wallet blocklisting increasingly ineffective as a standalone countermeasure.

Distributed Victimization Models

In response to newly implemented transaction caps and cooling-off periods, criminal networks are expected to scale distributed victimization approaches, sometimes referred to as smurfing-as-a-service. Rather than targeting a single individual for a large extraction, AI-coordinated bot networks direct hundreds of low-value transactions across dispersed kiosk locations simultaneously, keeping each transaction below regulatory thresholds while maintaining substantial aggregate revenue. This model complicates detection, as individual transactions appear unremarkable in isolation.

Hybrid Ransomware and Physical Payment Models

A projected longer-term development is the emergence of hybrid models in which crypto ATM kiosks become designated payment portals for ransomware attacks. In this scenario, victims of data encryption are instructed to make payment exclusively through physical kiosk deposits, introducing a mandatory in-person step that complicates the digital tracing methods typically used in ransomware investigations.



8. Recommendations

8.1 Consumers

Consumers should approach any unsolicited communication directing them to a crypto ATM with immediate skepticism. No legitimate government agency, law enforcement body, or financial institution will ever request payment or asset protection through a cryptocurrency kiosk. If contacted by someone claiming to represent such an entity, consumers should end the communication immediately and contact the organization directly using the phone number listed on its official website.

- Never send cryptocurrency to a wallet address provided by someone whose identity has not been independently verified through in-person contact or a trusted, separately initiated communication channel.

- QR codes received via text message, email, or social media may encode a wallet address controlled by a scammer. Do not scan QR codes from untrusted sources at a kiosk.
- If someone insists that you remain on a phone call while visiting a kiosk, this is a strong indicator of fraud. End the call immediately and consult a trusted person.
- Report any suspected crypto ATM fraud to the FBI's IC3 at ic3.gov, your local law enforcement, and the kiosk operator. If you have been victimized, contact your bank immediately and file a police report. While crypto transactions are generally irreversible, prompt reporting improves the probability that blockchain analytics firms can flag the destination wallet.
- Be aware that prior scam victims are frequently re-targeted with fraudulent recovery offers. Any contact claiming the ability to recover lost cryptocurrency for an upfront fee is itself a scam.

8.2 Operators

Crypto ATM operators occupy a critical position in the fraud pipeline and bear both regulatory and ethical responsibilities to minimize the exploitation of their infrastructure. The D.C. Attorney General's case against Athena Bitcoin has established that awareness of fraud without adequate remediation may expose operators to enforcement action under consumer protection and elder abuse statutes. Operators should implement the following measures:

- Deploy real-time on-chain monitoring that cross-references destination wallet addresses against known blocklists and law enforcement databases before executing any transaction.
- Implement tiered KYC verification proportional to transaction size, with mandatory government-issued identification for transactions exceeding $500 and enhanced due diligence for cumulative daily transactions exceeding $1,000.
- Install un-skippable, multi-language fraud warning screens that describe common scam scenarios in plain, non-technical language. These warnings should include explicit statements that no government agency, bank, or financial institution will ever require payment through a crypto ATM.
- Participate in industry-wide intelligence-sharing consortiums to ensure that wallet addresses and QR codes identified in fraud incidents at one operator's machines are blocked across all participating networks.
- Deploy behavioral analytics at the kiosk level, including monitoring for users on active phone calls, first-time users attempting maximum-threshold transactions, and users exhibiting visible signs of distress or confusion.

- Maintain 24/7 fraud reporting hotlines staffed by personnel trained to recognize and escalate potential fraud-in-progress situations.
- Disclose all transaction fees, markups, and service margins clearly and separately from the displayed exchange rate, in compliance with consumer protection requirements.

8.3 Law Enforcement

Law enforcement agencies at all levels should prioritize crypto ATM fraud as a high-impact financial crime category and invest in the specialized capabilities required to investigate and prosecute these cases across jurisdictions.

- Invest in blockchain analytics training and tooling, including platforms such as CertiK Skynet, to enable investigators to trace funds from the point of kiosk deposit through mixing and bridging services to eventual off-ramp endpoints.
- Establish dedicated crypto fraud task forces at the state level, modeled on the FBI's Virtual Currency Initiative, with subpoena authority over kiosk operator transaction records and coordination channels with international law enforcement through Interpol and Europol.
- Develop freeze-and-hold protocols with kiosk operators that enable rapid temporary holds on suspected fraudulent transactions while investigations are initiated.
- Create rapid-response referral pathways with Adult Protective Services and consumer protection agencies to ensure that elderly victims receive immediate support, including financial counseling and fraud recovery assistance.
- Advocate for federal legislation that standardizes reporting requirements, transaction caps, and operator licensing across all 50 states to eliminate the jurisdictional gaps that allow fraud networks to concentrate kiosk exploitation in states with minimal regulation.

9. Conclusion

Crypto ATM fraud represents a convergence of social engineering sophistication, regulatory fragmentation, and technological vulnerability that has created one of the fastest-growing financial crime categories in the United States. The $333.5 million in reported losses during 2025 reflects only a fraction of the actual harm, given well-documented underreporting and the devastating personal impact on victims, a disproportionate number of whom are elderly adults losing retirement savings.

The challenge is compounded by the international character of the criminal organizations involved, the speed at which stolen funds are moved beyond the reach of domestic law enforcement, and the structural incentives within the kiosk industry that have historically prioritized transaction volume over consumer protection. The Athena Bitcoin enforcement action signals a potential turning point in operator accountability, but systemic reform requires coordinated action across the technology, regulatory, and enforcement domains.

Effective intervention must operate at the ingress point, the narrow window between cash deposit and blockchain settlement, where real-time wallet screening and risk-calibrated transaction delays can disrupt the fraud pipeline before funds become irrecoverable. Upstream, sustained investment in public awareness remains essential, particularly for the demographic groups most frequently targeted. Downstream, standardized federal legislation, enhanced international cooperation, and continued development of blockchain forensic capabilities are necessary to close the jurisdictional and technical gaps that criminal organizations currently exploit.

The threat will continue to evolve. AI-augmented deepfakes, automated cross-chain laundering, and distributed victimization models will test the resilience of current countermeasures. The window for proactive intervention is narrowing. The organizations, technologies, and regulatory frameworks outlined in this report provide a foundation for disrupting the fraud pipeline, but only if the pace of defensive innovation matches or exceeds the rate of criminal adaptation.

Appendix: Data Sources and Methodology

This report draws on publicly available data and proprietary intelligence from the following sources:

- FBI Internet Crime Complaint Center (IC3): complaint and loss data for 2022 through November 2025
- Federal Trade Commission (FTC): consumer fraud reporting data and public advisories American Association of Retired Persons (AARP): victimology analysis and demographic data
- Chainalysis 2026 Crypto Crime Report: on-chain analytics, scam statistics, and money laundering network analysis
- CoinATMRadar: global crypto ATM market data and distribution statistics
- FinCEN: regulatory guidance and Bank Secrecy Act compliance alerts (August 2025 notice)
- District of Columbia Office of the Attorney General: Athena Bitcoin complaint and investigation data (September 2025)
- United Nations Office on Drugs and Crime (UNODC): Southeast Asian cybercrime and organized crime reporting
- CertiK Skynet: proprietary threat intelligence, wallet screening data, and operator interviews
- State legislative records and municipal ordinance databases for California, Florida, Vermont, Connecticut, Indiana, and Arizona

Quantitative data cited in this report reflects the most recent publicly available figures as of February 2026. Where multiple sources report conflicting figures for the same metric, the most conservative estimate has been used unless otherwise noted. Forward-looking projections in Section 7 are based on trend analysis of historical data, qualitative assessment of emerging threat indicators, and expert interviews, and should be understood as informed estimates rather than forecasts.

CERTIK
SKYNET

COMPANY INTRO

CertiK is the largest Web3 security services provider, founded in December 2017 in New York by two professors from Yale and Columbia University.

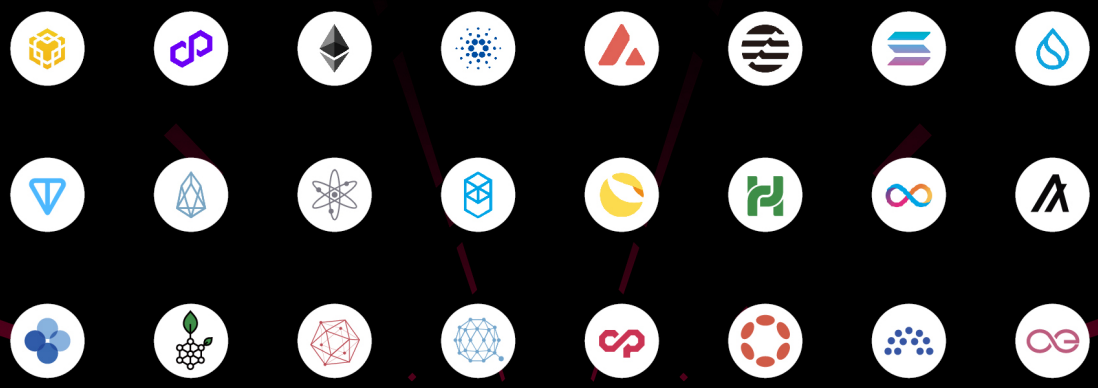
Powered by the industry's largest proprietary Web3 security database, CertiK provides actionable insights, including incident analyses, security reports and guidelines. It has also become a trusted security partner for global regulators, institutions, and Web3 enterprises, supporting both their security needs and their pursuit of innovation.

5,000+
CLIENTS SERVED

180,000+
VULNERABILITIES DETECTED

>$600B
MARKET CAP ASSESSED

>70% OF TOP 500 CMC PROJECTS AUDITED



DIVERSITY IN ECOSYSTEMS