State of New Jersey
Commission of Investigation

BITCOIN ATMs

Scams, Suspicious Transactions and Questionable Practices at Cryptocurrency Kiosks

February 2021

State of New Jersey
Commission of Investigation

BITCOIN ATMS

Scams, Suspicious Transactions and Questionable Practices at Cryptocurrency Kiosks

SCI
50 West State St.
P.O. Box 045
Trenton, N.J.
08625-0045
609.292.6767

www.state.nj.us/sci

Joseph F. Scancarella
Chair
Robert J. Burzichelli
Rosemary Iannacone
Kevin R. Reina
Commissioners

State of New Jersey

COMMISSION OF INVESTIGATION
50 WEST STATE STREET
PO Box - 045
TRENTON, NEW JERSEY 08625-0045
Telephone (609) 292-6767
Fax (609) 633-7366

Chadd W. Lackey
Executive Director

February 2021

Governor Phil Murphy
The President and Members of the Senate
The Speaker and Members of the General Assembly

The State Commission of Investigation, pursuant to N.J.S.A. 52:9M-1 to -20, herewith submits its final report of findings and recommendations stemming from an investigation into the operation of privately owned automated teller machines that facilitate the purchase or sale of cryptocurrency.

Respectfully,

Joseph F. Scancarella
Chair

Robert J. Burzichelli
Commissioner

Kevin R. Reina
Commissioner

Rosemary Iannacone
Commissioner

TABLE OF CONTENTS

Introduction

The Commission initially launched an inquiry into the operation of privately owned automated teller machines (ATMs) in New Jersey based upon allegations suggesting their use in facilitating illicit financial activity and other questionable practices. Subsequent investigation revealed improprieties related to a specific type of emergent machine known as Bitcoin ATMs, or kiosks, that allow customers to buy or sell cryptocurrency.[1]

The machines, which look similar to traditional ATMs and are often located near their familiar counterparts in coffee shops, convenience stores and other retail outlets, enable users to quickly and easily conduct cryptocurrency transactions. Yet, unlike regular ATMs, there is no state regulation of their operation in New Jersey, and the federal laws that are supposed to protect against money laundering and other financial crimes are complex**,** can be difficult to interpret and are not always enforced.

The Commission examined hundreds of records subpoenaed from 30 businesses that operated or were associated with approximately 300 cryptocurrency kiosks in New Jersey over the last five years and found instances where the machines were used to effectuate financial scams and to orchestrate questionable transactions.[2] Some transactions appeared arranged in a way that enabled users to circumvent machine requirements to produce a valid form of identification or to avoid triggering specific federal currency reporting rules. In many instances, the transactions should have been flagged by operators as indicators of potential criminal activity and reported to the federal government but were not.

Not only did the Commission discover wide variability in the precautions operators take – or fail to take – to safeguard against fraud, the inquiry also found inconsistencies among the various companies in how the businesses function, the type of information they collect from customers and the purchase limits for users. Lacking any government-sanctioned criteria for operation, business owners set their own rules for how much cryptocurrency users can buy, for the percentage charged for transaction fees – some were as high as 24 percent – and for the type of personal identifying information required to complete a sale.[3] Many machines permit near anonymity on purchases of up to $900 worth of cryptocurrency by allowing users to provide only a cellphone number. Some require no identifying information at all.

While the value of Bitcoin – the first and most widely used cryptocurrency – has fluctuated wildly in recent years, it hit a record high in February, trading above $50,000 per unit. As Wall Street's enthusiasm for Bitcoin has grown, so has the market for digital currency businesses, including the machines that enable in-person purchases of it.[4] Major corporations, including Microsoft, AT&T, Overstock.com and even Starbucks, now accept Bitcoin as a legitimate form of

---

[1] The machines are also known as BTMs.

[2] The Commission subpoenaed records from businesses operating in New Jersey from 2015 to 2020. Not all of the companies were operating at the time of the publication of this report.

[3] The Commission found wide disparity in transaction fees charged on the machines with rates typically ranging from eight to 20 percent. The rates often fluctuate based on market conditions.

[4] Many kiosks allow the purchase of various types of cryptocurrency.

payment.[5] As for the machines, only a handful existed when cryptocurrency kiosks first appeared in the United States in New Mexico in 2014, but now there are more than 11,665 nationwide.[6] Not only are the machines simple to operate, but they also offer investors a turnkey business opportunity with relatively cheap start-up costs and little overhead. Practically anyone with enough money – approximately $3,200 to $8,000 – and an Internet connection can buy a machine, plug it in and start doing business.[7]

Some of the qualities that make the machines appealing to users – their ease of use, the completion of transactions in real-time, and the ability to maintain a certain level of anonymity – also make them ripe for exploitation and criminal enterprise, such as money laundering. In July 2020, the Justice Department dismantled an unlicensed ATM network run by an owner/operator who admitted laundering between $15 to $25 million from in-person exchanges and transactions at his Bitcoin kiosks in California. A former bank employee, the operator admitted he knowingly laundered dirty cash, intentionally failed to register the business with the federal government and did not implement safeguards, such as conducting customer due diligence or filing reports on suspicious financial activity.

Across the nation, financial institutions and government agencies at all levels are wrestling with how best to oversee cryptocurrency and the various businesses related to its use.[8] The federal government treats cryptocurrency kiosks the same as banks and other financial institutions, requiring they follow precautions intended to protect the world's financial system from illicit use and money laundering. It generally does not pursue cases against unregistered entities or those that otherwise ignore the rules unless the business is involved in other criminality. Among the states, New York has implemented the most far-reaching regulation of the industry by requiring any individual or company that engages in virtual currency business activity to obtain a BitLicense. Some industry operators have criticized New York's stringent licensing process as too lengthy, burdensome and costly, particularly for smaller companies. As a result, some cryptocurrency businesses have come to New Jersey, where nearly no rules apply.

With expectations that the worldwide demand for cryptocurrency and the various applications of associated technology – such as blockchain – will only escalate, the industry will present financially enticing yet thoroughly unregulated avenues for legitimate and corrupt businesses alike.[9] To guide the growth of this burgeoning industry, safeguard it for customers, and protect it from the intrusion of unsavory elements, state government must establish proper and effective oversight of it. It is also essential that any regulation of cryptocurrency-related commerce strike a balance between creating fair and reasonable standards that enable

[5] While Starbucks does not accept cryptocurrency as a direct form of payment, it utilizes third-party apps that use or convert it.

[6] The total number of machines in the U.S. as of November 2020, according to Cointelegraph, an industry website.

[7] Models with additional features that allow users to buy and sell cryptocurrency can cost up to $14,500.

[8] In New Jersey, cryptocurrency is legal and is subject to sales or use tax.

[9] Blockchain is a digital ledger of records, called blocks, stored together as a chain and is often publicly accessible. The technology can be used to store information related to many other types of transactions outside of cryptocurrency, such as medical data, banking and real estate. In August 2019, Governor Phil Murphy signed bill S-2297 into law creating the New Jersey Blockchain Initiative Task Force to study potential uses for the technology.

businesses in that sector to prosper while guarding against fraud and efforts to corrupt the system.

Legislation pending in both houses, A-2891/S-3132, would address many of the Commission's core issues and concerns raised in this report. Among other things, the "Digital Asset and Blockchain Technology Act" would require any digital asset business to obtain a license from the State Department of Banking and Insurance (DOBI).[10] In its current form, the bill would establish a regulatory apparatus for the growing industry that provides consumer protections while also enabling businesses to operate without overly onerous restrictions. Though it would regulate a broad spectrum of entities that operate within the digital asset sphere – not only kiosks – the State should also implement specific requirements specifically related to the machines. Further detail about this recommendation and other proposals for statutory and regulatory reforms is presented at the end of this report.

Background

The Commission's inquiry primarily focused on devices, known as "unidirectional" machines, that enable customers to purchase cryptocurrency but do not offer the option to cash it out.[11] Users simply insert cash into the machine, agree to pay a transaction fee, and within moments purchase cryptocurrency at the market rate. Instead of receiving actual money, customers get a code that effectively unlocks the value of the cryptocurrency. Almost all cryptocurrency transactions can be viewed on a shared public ledger, known as the blockchain. Once redeemed, the cryptocurrency is stored in the customer's "wallet," which exist in various formats. Digital wallets allow users to store and retrieve their cryptocurrency through a cellphone app or a computer. Among the most basic of storage methods for cryptocurrency are paper wallets, which are pieces of paper that contain a code and a "key" that essentially enables customers to unlock access to their cryptocurrency.

Unlike transactions made directly through online exchanges – a common way to purchase cryptocurrency – kiosk customers do not need to provide a credit card or link to a bank account. Some machines do not even require users to create an account to conduct a transaction. Whereas transactions on an online exchange may take days to complete, those conducted on the machines are immediate.[12] Industry operators maintain the kiosks appeal not only to customers who want to keep their personal information private but also to those with no bank account, the underbanked or those who operate mainly with cash, such as service industry workers.[13]

[10] The primary sponsors of A-2891 are Assemblywoman Yvonne Lopez and Assemblyman Andrew Zwicker, both D-Middlesex, and Assemblyman Joe Danielsen, D-Somerset. Sen. Nellie Pou, D-Passaic, is the sponsor of S-3132.

[11] Some machines enable users to both buy and sell cryptocurrency.

[12] Fraud verification procedures performed by the exchange or the account holder's bank often cause delays.

[13] More than 22 percent of adults either do not have a bank account or are underbanked, according to a 2019 study from the Federal Reserve. Underbanked refers to those who may have a bank or checking account but utilize alternative financial services such as money orders, cash checking services or pawnshop loans. The unbanked and underbanked are more likely to have low incomes, less education, or belong to a racial or ethnic minority group.

While still unfamiliar to many consumers, the kiosks represent a small but steadily growing industry in New Jersey. A Commission review of records identified more than $70 million deposited into machines for cryptocurrency purchases between 2015 and 2020. Like the cryptocurrency market at-large, the ATM business is volatile, with operators and machines frequently entering and leaving the state. Still, overall deposits have roughly doubled annually in each of the last five years.

No state law applies directly to kiosk operators/companies except for the mandate that the entity – just as any other business that operates in New Jersey – register with the Treasury Department. Outside of that, the sole oversight of digital asset companies occurs at the federal government level. Cryptocurrency ATM/kiosk companies are considered money services businesses, and as such, must register with the Financial Crimes Enforcement Network (FinCEN) of the US Department of the Treasury. FinCEN is responsible for administering the Bank Secrecy Act, which requires banks, financial institutions and businesses involved in transmitting or accepting convertible virtual currency to file reports on transactions that are potentially indicative of money laundering.[14] Under the law, these entities are obliged to monitor transactions and file a Currency Transaction Report (CTR) for every payment, receipt or transfer of currency or monetary instruments totaling in excess of $10,000 per day for each customer.[15] Operators are supposed to collect identifying information on customers they do business with and perform other due diligence under "Know Your Customer" (KYC) regulations.[16] Further, if unusual customer activity or questionable transactions are discovered, the operator is required to submit a Suspicious Activity Report (SAR) to FinCEN.[17]

Even though entities that disregard these requirements are flouting federal law, the Commission found registration and report filing violations were not actively policed for operators in New Jersey.[18] While US regulators have mostly taken a passive approach to oversight, federal law enforcement authorities have cautioned that as the use of cryptocurrency evolves and expands, so too will opportunities to exploit the technology and commit crime. An October 2020 report from the US Attorney General's Cyber Digital Task Force noted that the failure of entities, including kiosk operators, to comply with the Bank Secrecy Act and other legal requirements threaten the agency's investigative abilities and undermine public safety.[19]

[14] Convertible virtual currency refers to virtual currency that has a value equivalent to currency, acts as a substitute for currency and is therefore a type of value that substitutes for currency.

[15] 31 CFR § 1010.311

[16] The Bank Secrecy Act was amended under the International Money Laundering Abatement and Financial Anti-Terrorism Act of 2001, also known as the Patriot Act, to require entities to provide customer identification information and monitor customers' habits and flag unusual activity.

[17] 31 CFR § 1022.320

[18] Under 18 U.S.C. § 1960, any person found guilty of operating an unlicensed MSB can face up to five years in prison. In addition, an unlicensed operator could also be liable for a civil penalty of $5,000 for each violation under 31 U.S.C. § 5330 and 31 CFR § 103.4.

[19] *Cryptocurrency: An Enforcement Framework* was the third and final report from the federal task force.

Key Findings

In its review of cryptocurrency machines, the Commission found areas of concern that legislators, law enforcement, and the public should be aware of as New Jersey considers measures to regulate elements of this swiftly expanding industry.

No ID Required

By permitting even a portion of transactions to occur anonymously, ATM operators leave the machines vulnerable to abuse by those who want to exploit the technology for nefarious purposes. Without capturing verifiable identifying information on its customers, their cryptocurrency transactions on the devices are virtually untraceable, which puts law enforcement at a distinct disadvantage when conducting investigations into suspicious activity.

A Commission analysis found the vast majority of companies that operate machines in New Jersey enabled users to conduct at least some transactions anonymously. Among the findings:

- Nearly 75 percent of the companies allowed certain transactions to proceed without requiring the user to present any information outside of a cellphone number.[20]
- More than half of those businesses permitted users to purchase up to $900 worth of cryptocurrency with only a cellphone number or no information at all.
- Security measures were stricter for larger purchases, with 87 percent of all companies requiring additional identification, such as Social Security number, ”selfies,” or tax ID for purchases exceeding $3,000.[21]
- Only 25 percent of businesses required buyers to provide a valid form of identification for every purchase.

Capturing cellphone information is an exceedingly unreliable method for verifying an individual's identity. Legitimate customers may use cellphones not registered under their own names but in an account in the name of a spouse or other relative. Individuals involved in criminal activity sometimes use pre-paid cell phones, known as “burners” or “throwaways” because they leave no trail back to the user. Typically purchased with cash, the phones require no proof of identification from the buyer and are disposed of once the pre-paid time expires. Unscrupulous individuals also often utilize so-called “burner numbers,” which are second phone numbers that can be purchased online and used on any cellphone. Just as it is with throwaway phones, purchasers of burner numbers select any available area code and phone number, making it difficult to trace back to a given individual.[22]

[20] The Commission reviewed machine settings and specific business practices for 16 ATM operators known to be operating in New Jersey in 2020.

[21] Many machines are equipped with cameras that take a photo of the user that are referred to as ”selfies.” Some require the customer to hold up a form of government identification in the photo.

[22] The Commission identified a handful of companies that prohibit the use of Voice over Internet Protocol (VoIP) phones to conduct machine transactions. VoIP uses an Internet connection instead of a landline or mobile network.

Even companies that appeared to be otherwise diligent about monitoring and reporting suspicious activities permitted purchases that necessitated the user to furnish only a cellphone number. The Commission uncovered examples in which customers conducted several smaller transactions in a short time frame, enabling the users to dodge machine requirements to produce a valid form of identification for larger purchases. The smaller transactions also often skirt the $2,000 threshold that triggers the operator to file a SAR. The failure to capture identifying information on users for *all* machine activity means that even operators that are appropriately watching the transactions and informing FinCEN of questionable events do not truly know their customers.

A North Jersey-based operator told the Commission the company routinely monitored transactions and filed the appropriate reports to federal authorities if any activity appeared unusual. The company also utilized cameras on the machines to monitor customer activity. But the company knows nothing about customers who make purchases of less than $800 – outside of the cellphone number supplied by the user – a practice that effectively undermines its efforts to conduct thorough customer due diligence. The operator testified the company appropriately filed SARs after machine photos showed the same individual conducted a series of $800 transactions. However, the report would have provided little useful information to law enforcement authorities due to the lack of reliable identifiers for the customer.

Digital Mint, a larger Chicago-based company with three dozen machines in New Jersey, decided in 2016 to require customers to provide identification for all transactions after an internal audit found cellphone data was not adequate to meet FinCEN requirements. Although some customers initially complained and business briefly dropped off, those setbacks had no long-term impact on the company's bottom line, according to sworn testimony from its co-owner.

Questionable Compliance

The Commission found wide disparities among the 30 businesses operating cryptocurrency kiosks related to registration with state and federal agencies as well as their implementation of anti-money laundering controls. While most entities properly registered their business with the State of New Jersey, nearly a third failed to register to operate here legally.[23] In addition, more than a third of the companies did not register with FinCEN as money services businesses.[24]

Of the non-compliant entities, some willfully disregarded requirements to register their businesses and made no effort to monitor transactions or to implement practices that enable operators to know their customers. Others claimed total ignorance of the federal mandate to file SARs or report activity that could indicate money laundering. Moreover, some owners/operators

[23] In New Jersey, a business can be voided or revoked for the failure to file annual reports for two consecutive years or for the failure to file corporation business taxes.

[24] Not every business that did not register with the State also failed to register with the federal government. Six companies never filed with the State or FinCEN.

appeared to lack even a basic understanding of how the machines operated and insisted the manufacturer took care of anti-money laundering reporting obligations.

In sworn testimony before the Commission, Noel Harvey, the owner/operator of six machines in Bergen, Hudson and Morris counties, acknowledged he never registered Crypto Cash ACM – the name used for his kiosk business – or its parent company, SEVEC LLC, with FinCEN.[25] He never filed paperwork to flag questionable transactions or conducted customer due diligence either, claiming the manufacturer handled those matters. During his testimony, Harvey appeared unfamiliar with rudimentary procedures for the machines. He admitted being aware of financial schemes conducted through the company's devices but did not report the incidents to law enforcement. He also did not know whether certain transactions required the user to submit a phone number. When Commission counsel asked if he filed state or federal taxes for the business, Harvey exercised his constitutional right of protection under the Fifth Amendment against possible self-incrimination.

A review of transactions conducted at four of Harvey's terminals between April and September 2019 revealed several instances of transactions with purchases exceeding $10,000 – occasions that should have resulted in the filing of a report alerting FinCEN to questionable and possibly illicit activity. On one of those occurrences, a series of ten transactions – each for $1,000 that were sent to the same wallet – occurred in the span of a few minutes. The transactions appeared arranged in a way to evade the $10,000 daily customer threshold that triggers the filing of a CTR. At the very least, a vigilant operator should have alerted FinCEN that the purchases appeared suspicious. But that never happened because at Harvey's machines, identifying details about customers were not routinely collected, transactions were not reviewed, and no information was reported to FinCEN. Harvey testified that he did not know what, if any, identification the user was asked to provide for those purchases.

Harvey testified his initial exposure to the industry came from attending a cryptocurrency conference held in 2017 by a company later shut down by the Securities and Exchange Commission for running a pyramid scheme. Outside of that, his knowledge of the ATM business came from watching YouTube videos and from paid consultant Frank Robertson – a seven-time convicted felon with a long history of financial-related crimes who once co-owned a business, 2Nickles, that operated a handful of machines in North Jersey that were never registered with the state or FinCEN. Recently convicted of federal fraud charges, the Commission found evidence Robertson is back in the ATM business unlawfully operating two machines in Hudson County.

In October 2019, when SCI agents visited the gas station where one of the machines is located, a station employee identified Robertson as the individual who placed the kiosk there and serviced it. Robertson’s contact information appeared at the top of a contract between an entity called Near By Coins ACM and the store owner to house the terminal. While the agreement was unsigned, the owner told investigators Robertson paid him $200 a month to lease the space.

[25] Records reviewed by Commission staff indicate SEVEC subsequently registered with FinCEN in September 2020, several months after Harvey's testimony before the Commission. Harvey previously registered SEVEC LLC, which operated as a parking company, as a business in New Jersey, but the company remains in suspended status due to the failure to pay the annual fee.

Meanwhile, there is no record of registration for the business with either the State of New Jersey or FinCEN.

When asked about his cryptocurrency-related activities during sworn testimony before the Commission, Robertson refused to answer questions concerning these matters, citing his Fifth Amendment privilege against self-incrimination. During the investigation, the Commission obtained evidence indicating certain operators, including Robertson and Harvey, worked under the belief that the machines – not the operator – took care of flagging questionable transactions and reporting such activity to authorities.

General Bytes, one of the largest manufacturers of Bitcoin kiosks and the company that sold machines to both Robertson and Harvey, told the Commission the devices it sells do not perform any anti-money laundering compliance functions. In a September 2020 email to the SCI, the owner of the Czech Republic-based company further wrote:

> *Yes, we instruct customers to consult with their local lawyers and accountants what their responsibilities are. Giving other, a more specific advises [sic] may mislead customer. We are ATM manufacturer. We sell ATMs all over the world. We do not want to pretend that we are competent to give legal advises [sic] to companies. Crypto-currency regulation is different in every country and changes every 6 months. We believe that our customers understand that they need MSB licenses and similar and know what their responsibilities are.*

While some operators knowingly violated the rules, others professed ignorance concerning their obligations to register their business with FinCEN and comply with anti-money laundering mandates. The owner/operator of a lone machine in Fort Lee, who at the time had been in business less than a year, claimed to be completely unaware of the need to register with the federal government as a money services business until he was advised of this requirement by Commission agents.[26] In response to a Commission subpoena requesting information on whether he had discovered or reported any suspicious financial activity on his machine, the owner/operator wrote:

> *This is actually the first time I became aware of SARs and its purpose. As reporting any SARs is required to be submitted within a specific timeframe [sic] I have not experienced any recent fraud or scam. However moving forward, I will document and report any suspicious activity to FinCen [sic].*

Similarly, the owner/operator was unfamiliar with currency transaction reports.

> *Unfortately[sic], same as SARs, I did not have any knowledge CTRs and it's [sic] purpose. Moving forward, I will document and report any currency transactions in excess of $10,000 to FinCen [sic].*

[26] The owner/operator has since registered with FinCEN as an MSB and hired a certified anti-money laundering specialist and fraud examiner to advise his business.

A Commission review of transactions at the machine between July 2018 and June 2020 revealed that $206,000 flowed through the device during that time without any monitoring by the operator to comply with KYC and anti-money laundering laws.[27] Equally troubling, no identifying information was captured for any of the customers in those transactions.

Based on the Commission's review, it is clear that operators in New Jersey are not consistently or committedly complying with reporting mandates and that absent greater conformity, the kiosks remain vulnerable to abuse and criminal intrusion. These findings reinforce warnings from the Justice Department that businesses that avoid compliance with anti-money laundering standards and KYC requirements provide opportunities for criminals to hide their illicit financial gains from regulators and criminal investigators.

Fraudulent Schemes

In addition to their use as vehicles for questionable transactions, criminals also utilize cryptocurrency kiosks to carry out various types of fraudulent schemes.[28] The Commission uncovered numerous instances where unwitting victims were duped into sending cryptocurrency to unknown wallets through the machines, including some schemes that resulted in the loss of tens of thousands of dollars. Cryptocurrency transactions are irreversible, leaving victims with no way of recovering the lost funds.

By monitoring activity at the machines, diligent operators can halt schemes from progressing, or at the very least, flag suspicious transactions and alert federal authorities to activity potentially indicative of further misconduct. To their credit, some ATM companies have developed proactive strategies to inform customers about potential fraud and required users to review a disclaimer outlining the risks associated with cryptocurrency before commencing any transactions. Others have placed stickers on the machines warning customers of scams and urged users to alert operators to requests from third parties to send cryptocurrency to them. The Commission identified several companies that required customers to certify the wallet where the virtual currency was sent belonged to them and not someone else. Some operators, such as BelcoBTM, have cultivated employees in the stores that house machines to keep an eye out for suspicious activity or unfamiliar users.

Companies that discover individuals using their machines to engage in inappropriate activities also have the ability to ban those customers from the kiosks or to block certain wallets. An SCI review of company records found more than 900 customers or wallets that were either banned or blocked by 10 companies with kiosks in New Jersey. Operators banished individuals

[27] The machine is unlike most of the terminals located in New Jersey as it permits both the purchase and sale of cryptocurrency.

[28] The Justice Department has also linked the kiosks to unlawful conduct by drug dealers, credit card schemers and prostitution rings.

from their machines for various reasons, including the utilization of multiple wallets, using Bitcoin obtained on the machine to fund Darknet purchases or for an association with a scam.[29]

Among the schemes identified by the Commission:

- Cryptocurrency kiosks were utilized to carry out a scam that duped multiple victims into spending a total of more than $600,000 to buy vehicles advertised for sale on eBay but did not really exist. Under the scheme, purchasers wire transferred money intended for the vehicle acquisition to a particular bank account. After receiving the money, an individual working for the scammer would take the funds, purchase bitcoins through various kiosks in New York City and New Jersey, and then send it to designated wallets controlled by the scam artists. From October 2016 to March 2017, this individual purchased more than $170,000 in bitcoin at a Lyndhurst kiosk alone. Law enforcement learned about the scheme after a victim contacted a bank where money was wired and reported never receiving a vehicle. Ultimately, the New Jersey State Police arrested and charged the individual with various crimes, including theft by deception, money laundering and deceptive business practices.

- In April 2019, a caller identifying himself as both an agent with the Federal Trade Commission and a U.S. Marshal informed the victim that her identity had been stolen. The caller claimed two properties in Texas that authorities suspected were linked to money laundering activity and drug trafficking were purchased in the victim's name. In addition, the caller told the victim her Social Security number was used to open four bank accounts. The scammer warned the victim that all her bank accounts would be frozen pending further investigation, but she could "prove her innocence" if she moved money from her bank accounts, converted it to cryptocurrency and transferred it to an allegedly secure federal account already set up. The victim had 40 minutes to drain her accounts and visit seven different cryptocurrency kiosks in Bergen, Essex and Passaic counties to deposit the money into a secured "federal account." After completing the final transaction at an ATM in Clifton, a store associate approached the victim and asked where she was sending the money. The store worker had received a call from an employee of the machine's operator, who was aware of the prevalence of scams and knew the woman was not a regular customer based on real-time monitoring of the transactions. In total, the woman lost $12,000 in the scam.

- In July 2019, a customer contacted the owner/operator of a Fort Lee machine to report a fraud in which an unknown caller requested the victim to use the terminal to send $8,000 in bitcoin, broken down into smaller increments of $500, to a specific wallet.[30] After sending the money, the victim realized it was a fraud and reported the incident to the owner/operator.

[29] The Commission found two ATM companies banned a Staten Island man from using their machines after discovering he purchased bitcoin that was later sent to offshore gambling websites.

[30] The scammer likely requested the victim to purchase the $8,000 in smaller amounts in order to avoid triggering KYC reporting requirements.

- In September 2019, a victim reported receiving a call from a caller identified as a Public Service Electric and Gas employee who demanded payment for an outstanding debt that, if not resolved, would result in legal action against the target. The caller instructed the victim to purchase $450 in bitcoin at the Fort Lee cryptocurrency machine and send it to the address provided by the scammer. After completing the transaction, the victim grasped the scheme and contacted the owner/operator inquiring about whether the lost funds were recoverable, but was told all transactions are irrevocable.

Recommendations

Under current laws and regulations, New Jersey has no authority over the burgeoning cryptocurrency industry. As demonstrated by the findings in this report, the lack of oversight of machines that enable users to purchase significant amounts of cryptocurrency practically anonymously renders them vulnerable to abuse by bad actors who seek to exploit the technology for illicit purposes. Without any state regulation of their operation, no protections exist for consumers unfamiliar with the fast-moving terrain of cryptocurrency transactions and fall victim to scams. Further, there are no standards to ensure operators of these businesses function in a reliable, consistent and transparent manner.

As indicated earlier in this report, pending legislation, A-2891/S-3132, would address a number of the concerns raised by the Commission by creating a licensing mechanism for individuals who engage in a digital asset business activity, including cryptocurrency kiosks.[31] An applicant for licensure would be required to disclose any criminal convictions or pending criminal charges against either the business's primary operator or top officers. Further, it also would require the disclosure of any ongoing litigation, a bankruptcy filing within the prior ten years or a license revocation or suspension in another state. Under the measure, any individual who operates a digital asset business without a license would face a fine of $500 per day.

To protect consumers, the bill requires the disclosure – "in readily understandable language" – of the terms and conditions of a customer's account with the business regarding fees or charges, potential risks and any protections and securities in place. A customer would need to agree to the terms set out in the disclosure before any transaction or digital asset balance inquiry commenced at a kiosk.

In addition to enacting this legislation, decision-makers should consider – either as an amendment to the bill or by department regulation – expanding the period for record retention beyond the one year proposed, and instead applying the same standard that pertains to businesses in the banking industry. In New Jersey, banks and financial institutions must retain records of accounts, including transactions, for six years.[32] Limiting access to only a twelve-month window could constrict the ability of law enforcement and regulators from obtaining a larger

[31] The legislation would also honor licenses held by operators or businesses in a state with a reciprocity agreement with New Jersey.
[32] N.J.S.A. 17:16W-3

volume of information needed to investigate incidents of suspicious financial activity. At a minimum, the criteria should match those under the Bank Secrecy Act, which requires money services businesses to retain records related to transactions for five years.

While the proposed legislation requires disclosure of an applicant's criminal history, the Commission recommends the DOBI Commissioner apply greater scrutiny to any individual convicted of a crime of moral turpitude involving dishonesty, fraud or deceit within the past ten years. During the inquiry, the Commission identified two individuals with recent federal convictions for financial-related crimes whose ATM companies engaged in various questionable business practices.

Concerning the operation of the machines, it should be mandated that all machine customers provide a valid form of government-issued identification with a photo before any transaction can proceed. Requiring IDs for all purchases ensures that every transaction on a device is traceable to a specific individual. Without identifying information on users, law enforcement's investigative capabilities remain hamstrung when probing suspicious transactions and potential links to criminal activity. The Commission identified several cryptocurrency businesses that have taken the lead in this area and already require customers to provide government-issued IDs for all transactions.[33]

[33] In addition to Digital Mint, the Commission found three other companies with machines in New Jersey – Coinlinx, Coinsource and Byte Federal – all require customers to present valid government-issued identification before a transaction can proceed.

State of New Jersey
Commission of Investigation