Whitepaper

# Anatomy of a Fraudulent Deposit: Account Activity Patterns Behind America's Check Fraud Surge

David Maimon

SentiLink | VALID systems

# Anatomy of a Fraudulent Deposit: Account Activity Patterns Behind America’s Check Fraud Surge

# Executive summary

Since mid-2021, check fraud in the United States has evolved from opportunistic “check washing” to a scaled, technology-enabled enterprise rooted in mail theft and powered by digital “check cooking.” This white paper focuses on the destination accounts to which these fraudulent checks are deposited — who controls them and how they behave before fraud.

Drawing on four years of threat-intel collection and casework by SentiLink, plus more than two decades of transactional analysis expertise by VALID Systems, we examined 104 stolen checks posted in fraud markets. Two account-owner types dominate: (1) fraudster-controlled accounts opened with stolen or synthetic identities, and (2) legitimate customers who are either deceived into participating or collaborate for a cut.

Critically, fraudulent deposits span the account lifecycle: new (33%), young 2–6 months (22%), aging 7–12 months (7%), and tenured 1+ years (37%). While new-account fraud remains voluminous—and highly detectable—older accounts present the greater strategic risk: consistent, legitimate activity builds trust, after which a large anomalous check lands with fewer alarm.

The following behavioral signatures were observed for each account age segment:

- **New (<30 days):** These accounts carried an average 4-week balance of about $1,000 and showed 2–3 small legitimate deposits under $2,000 — followed by an average fraudulent check of $4,288.
- **Young (2–6 months):** These accounts carried relatively low balances of around $300 and showed legitimate deposits averaging $1,400 — followed by a fraudulent check averaging $3,635.
- **Aging (7–12 months):** These accounts carried an average 4-week balance of about $1,300 and showed rising legitimate deposits averaging $2,500 — followed by a fraudulent check averaging $5,746, often issued by reputable payers.
- **Tenured (≥1 year):** These accounts carried an average 4-week balance above $5,000 and showed steady legitimate deposits exceeding $2,500 per month — followed by a fraudulent check averaging $8,277. Notably, many of these account holders were actually scammed customers.

**What this means:** Check fraud is no longer a legacy nuisance; it is a modern supply chain crime that blends identity fabrication, account brokering, and social engineering. Traditional controls that equate account age with safety underestimate the risk. The most effective defenses pair identity intelligence with behavioral trend analytics and payer-level signals, and they operate across institutions, not in silos.

**Bottom line:** The fraudsters' advantage is coordination and patience. Institutions that match it with multi-layer analytics, cross-industry visibility, and customer protection at the core will cut losses, protect victims, and disrupt the stolen-check economy at scale.

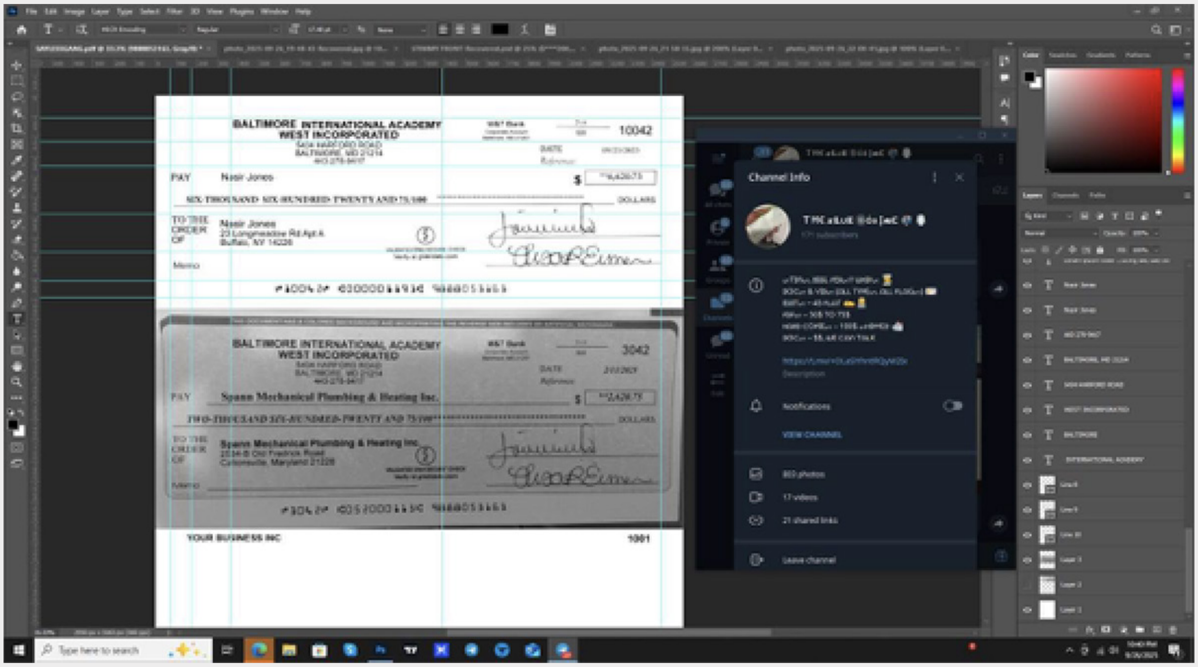
# Check theft and check fraud background

Check theft and fraud in the United States have evolved since mid-2021 into a sophisticated criminal enterprise rooted in mail theft. Offenders frequently target residential mailboxes and USPS blue collection boxes, often using stolen or duplicated USPS "arrow keys" to gain access to outgoing mail. Once the mail is collected, it is transported to a designated hideout where accomplices sort through the stolen envelopes in search of checks.

Initially, these criminals relied on rudimentary "check washing" methods — using chemicals such as nail polish remover or acetone to erase payee and amount information before rewriting checks to inflate their value or redirect funds to themselves or their associates. However, the scheme has since advanced into what is now known as "check cooking."

"Check cooking" involves digitally extracting the original check's signature and other authentic elements, then using image-editing tools — traditionally software like Photoshop — to fabricate entirely new, highly convincing counterfeit checks. But the technique has evolved rapidly. Today, fraudsters increasingly rely on AI-driven image generation and deepfake-style manipulation to recreate check layouts, handwriting, and security features with stunning accuracy. These models can generate or alter check images that are nearly indistinguishable from genuine ones, even under close inspection.

As a result, detecting cooked checks has become dramatically more difficult for both victims and financial institutions. Visual cues that once reliably signaled tampering — irregularities in font, spacing, shadows, or backgrounds — can now be replicated or corrected algorithmically. With AI enabling high-quality forgeries at scale, the verification challenge grows substantially, giving fraudsters a powerful new advantage in check-based schemes.



BALTIMORE INTERNATIONAL ACADEMY
WEST INCORPORATED

10042

PAY Nasir Jones $ 6,620.75

SIX THOUSAND SIX HUNDRED TWENTY AND 75/100 DOLLARS

TO THE ORDER OF Nasir Jones
23 Longmeadow Rd Apt A
Buffalo, NY 14226

Memo

BALTIMORE INTERNATIONAL ACADEMY
WEST INCORPORATED

3042

PAY Spann Mechanical Plumbing & Heating Inc. $ **2,620.75

TWO-THOUSAND SIX-HUNDRED-TWENTY AND 75/100 DOLLARS

TO THE ORDER OF Spann Mechanical Plumbing & Heating Inc.
2034-B Old Fredrick Road
Catonsville, Maryland 21228

Memo

YOUR BUSINESS INC 1001

Channel Info

Notifications

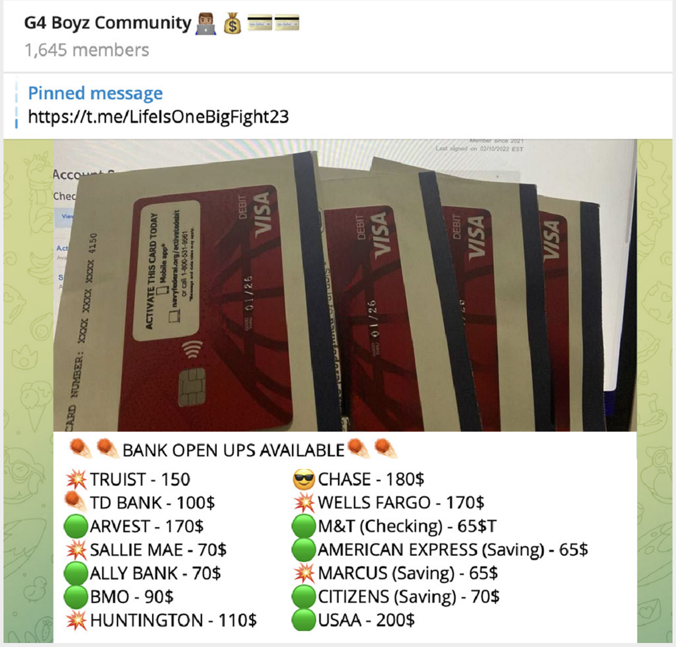
VIEW CHANNEL

Leave channel

*Screenshot of check cooking in progress*

With the checks in hand, criminals typically keep a portion for themselves and sell the remainder on online fraud marketplace channels that have included Telegram, WhatsApp and even Facebook. To convert stolen checks into cash, they initially relied on recruited “mules” — often older adults, people with substance-use disorders, or unhoused individuals — who were given specific instructions for presenting and cashing the checks. As the volume of stolen checks grew around early 2023, fraud rings moved toward creating “drop” bank accounts to receive deposits and withdraw funds more easily. In response, the online fraud economy developed services that create and age bank accounts for resale, with prices reported as low as roughly $150 for newly opened accounts and up to about $1,000 for accounts aged six months.

The ready availability of stolen checks, coupled with services for identity fabrication, document creation, and bank account opening, has transformed check fraud into a lucrative enterprise controlled primarily by domestic crime syndicates. Within these operations, different actors specialize in distinct stages of the stolen-check supply chain, from mail theft to cash-out. These interconnected components also help explain the sharp rise in check fraud reports submitted to FinCEN beginning in 2021, as well as the persistently high reporting volume since then.



G4 Boyz Community 👨🏽‍💻 💰 💳💳
1,645 members

Pinned message
https://t.me/LifeIsOneBigFight23

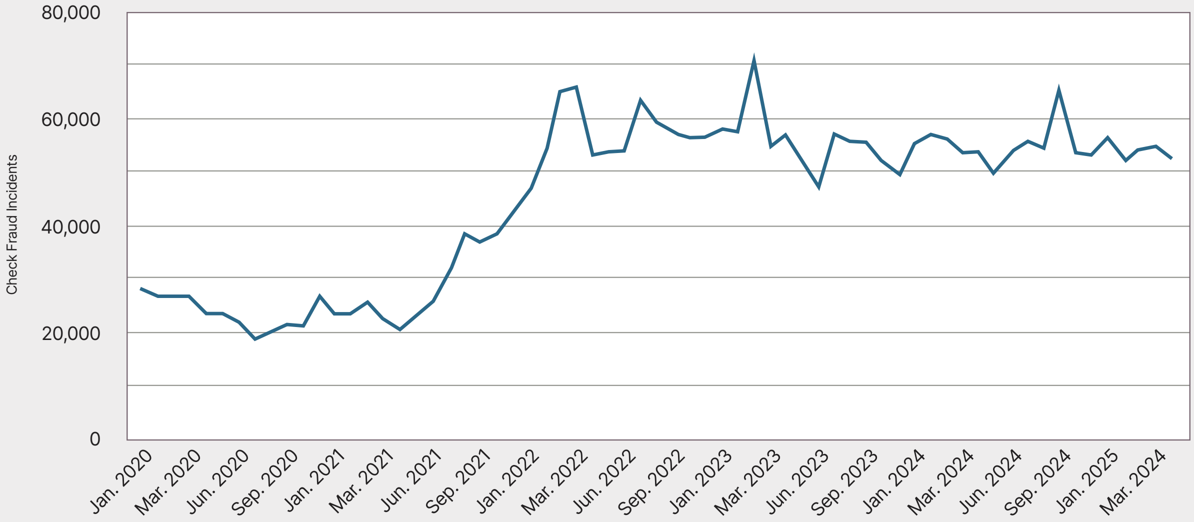
☄️ ☄️ BANK OPEN UPS AVAILABLE ☄️ ☄️

💥TRUIST - 150
☄️TD BANK - 100$
🟢ARVEST - 170$
💥SALLIE MAE - 70$
🟢ALLY BANK - 70$
🟢BMO - 90$
💥HUNTINGTON - 110$

😎CHASE - 180$
💥WELLS FARGO - 170$
🟢M&T (Checking) - 65$T
🟢AMERICAN EXPRESS (Saving) - 65$
💥MARCUS (Saving) - 65$
🟢CITIZENS (Saving) - 70$
🟢USAA - 200$

DEBIT
VISA
ACTIVATE THIS CARD TODAY
CARD NUMBER: XXXX XXXX XXXX 4150
01/26
Member since 2021
Last signed on 02/10/2022 EST

*Bank account creation services offered on Telegram*



*Monthly check fraud incidents reported to FinCEN between 2020-2025**

Beyond direct financial losses, stolen checks have become a gateway to broader identity fraud. Our research indicates that criminals frequently exploit victims' personal information — names, addresses, and other identifiers — to forge driver's licenses, passports, and other identity documents. These falsified credentials, in turn, enable more complex schemes such as fraudulent credit applications and account takeovers.

Over the past four years, we spent considerable time mapping the supply chain of check theft and check fraud and so we now have a clear picture of how the check theft and fraud ecosystem operates. Yet one critical piece remains relatively under-explored in the public domain: the bank accounts into which stolen checks are deposited. Who controls those accounts, and what patterns of financial activity, if any, occur in them prior to a fraudulent deposit?

Some financial institutions may be able to answer parts of this question, but many lack the resources or cross-institutional visibility to do so. Moreover, while analyzing data in isolation is useful, combining data across multiple financial institutions can reveal patterns that single-institution analyses miss. That's why we partnered with Valid Systems, a decision intelligence company who processes check transactions for 8 of the top 25 FIs and has cross-institution visibility and pattern recognition advantage.

Therefore, the goals of this paper are twofold. First, we seek to answer: who owns the accounts used to receive stolen-check deposits? Second, we ask: what does a typical sequence of account activity look like in the days and weeks before a fraudulent check is deposited?

# Who controls the accounts receiving stolen-check deposits?

To identify who controls the bank accounts used to deposit stolen checks, we rely on data we collected and analyzed from online Telegram markets advertising stolen checks and check-fraud services during the last four years. In many cases, alongside images of the stolen checks, sellers also post photographs of ATM deposit slips to boost potential buyers' confidence in the legitimacy of their offerings. Because these images often display information from both the checks and the deposit transactions, they could be shared with victims or financial institutions to help prevent or trace fraudulent activity. Our conversations with victims and financial institutions with whom we have shared many images of stolen checks and ATM deposit slips, coupled with investigative use of our analytical tools, point to two main types of account owners involved in these schemes:

1. Fraudsters who open accounts using stolen or synthetic identities.

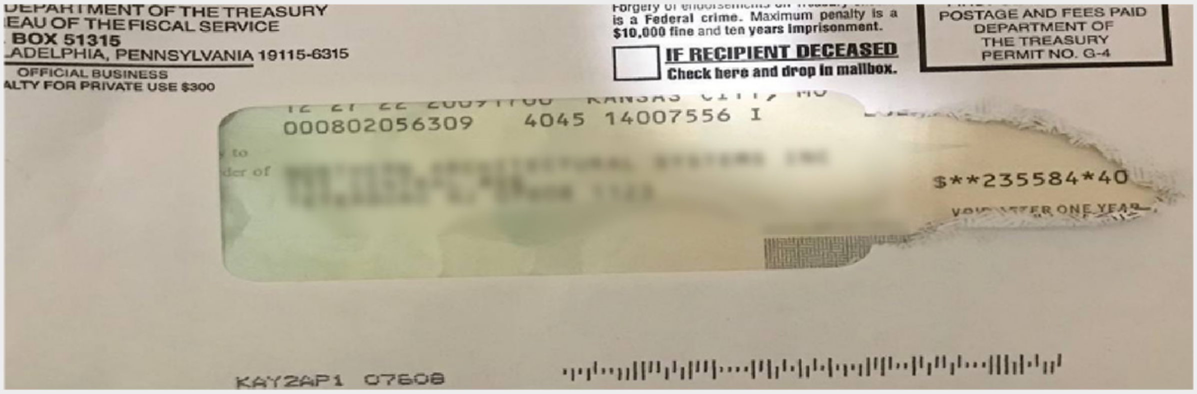
2. Legitimate account holders who either collaborate willingly with the fraudsters or are manipulated into participating, often through deception or financial inducement.

The distinction between these two account-owner types becomes even clearer when viewed through real cases. The next section highlights several examples that demonstrate how both fraudulent and legitimate account holders contribute — knowingly or not — to sustaining the check-fraud supply chain.

# Fraudsters who use stolen and synthetic identities to open bank accounts

Criminals frequently open new bank accounts using stolen identities. They acquire personal information from online fraud markets and data-breach archives, then forge or purchase counterfeit driver's licenses and other identification documents. These credentials enable them to open accounts at traditional banks and fintech institutions under victims' names.

A SentiLink investigation into two stolen checks identified in early 2023 offers a clear illustration of this modus operandi, highlighting the methods fraudsters use to establish and operate accounts created with stolen or synthetic identities. The investigation began when our team identified two unusually high-value checks, issued by the U.S. Department of the Treasury as tax refunds to a business owner, being advertised for sale on one of the Telegram markets we monitor. Due to the large amounts involved, we contacted the business owner to alert him.



DEPARTMENT OF THE TREASURY
EAU OF THE FISCAL SERVICE
BOX 51315
ADELPHIA, PENNSYLVANIA 19115-6315
OFFICIAL BUSINESS
ALTY FOR PRIVATE USE $300

Forgery or endorsements on Treasury checks is a Federal crime. Maximum penalty is a $10,000 fine and ten years imprisonment.

□ IF RECIPIENT DECEASED
Check here and drop in mailbox.

POSTAGE AND FEES PAID
DEPARTMENT OF THE TREASURY
PERMIT NO. G-4

KANSAS CITY, MO

000802056309 4045 14007556 I

to
der of [redacted]

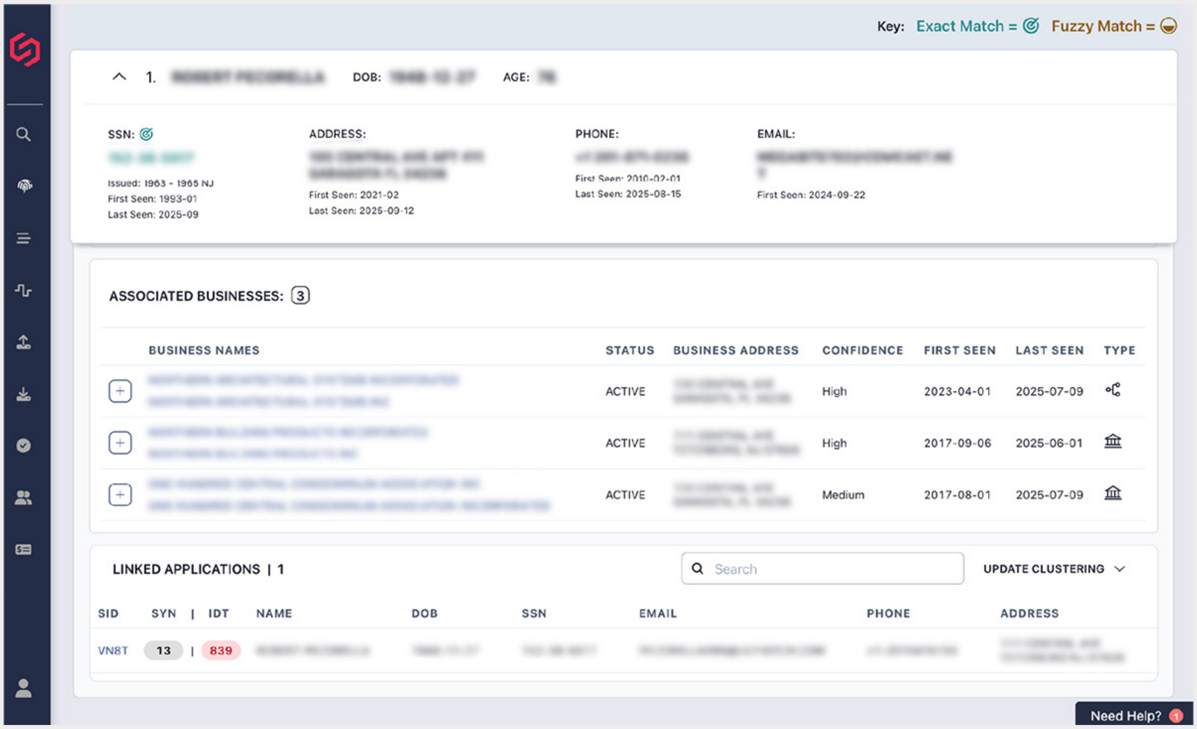
$**235584*40

VOID AFTER ONE YEAR

KAY2AP1 07608

*Stolen U.S. Department of Treasury Check Mailed to New Jersey Address, Used to Open a Bank Account with a Stolen Identity*

SentiLink investigation revealed that the victim's identity was used to apply for a new bank account around the same time the stolen checks appeared. The application showed multiple red flags: it originated from a suspicious IP address, and it listed an email account created only a few days before submission.



Key: Exact Match = ◎ Fuzzy Match = ◒

1. [redacted] DOB: [redacted] AGE: [redacted]

SSN: ◎
[redacted]
Issued: 1963 - 1965 NJ
First Seen: 1993-01
Last Seen: 2025-09

ADDRESS:
[redacted]
First Seen: 2021-02
Last Seen: 2025-09-12

PHONE:
[redacted]
First Seen: 2010-02-01
Last Seen: 2025-08-15

EMAIL:
[redacted]
First Seen: 2024-09-22

ASSOCIATED BUSINESSES: 3

| | BUSINESS NAMES | STATUS | BUSINESS ADDRESS | CONFIDENCE | FIRST SEEN | LAST SEEN | TYPE |
|---|---|---|---|---|---|---|---|
| + | [redacted] | ACTIVE | [redacted] | High | 2023-04-01 | 2025-07-09 | |
| + | [redacted] | ACTIVE | [redacted] | High | 2017-09-06 | 2025-06-01 | 🏛 |
| + | [redacted] | ACTIVE | [redacted] | Medium | 2017-08-01 | 2025-07-09 | 🏛 |

LINKED APPLICATIONS | 1

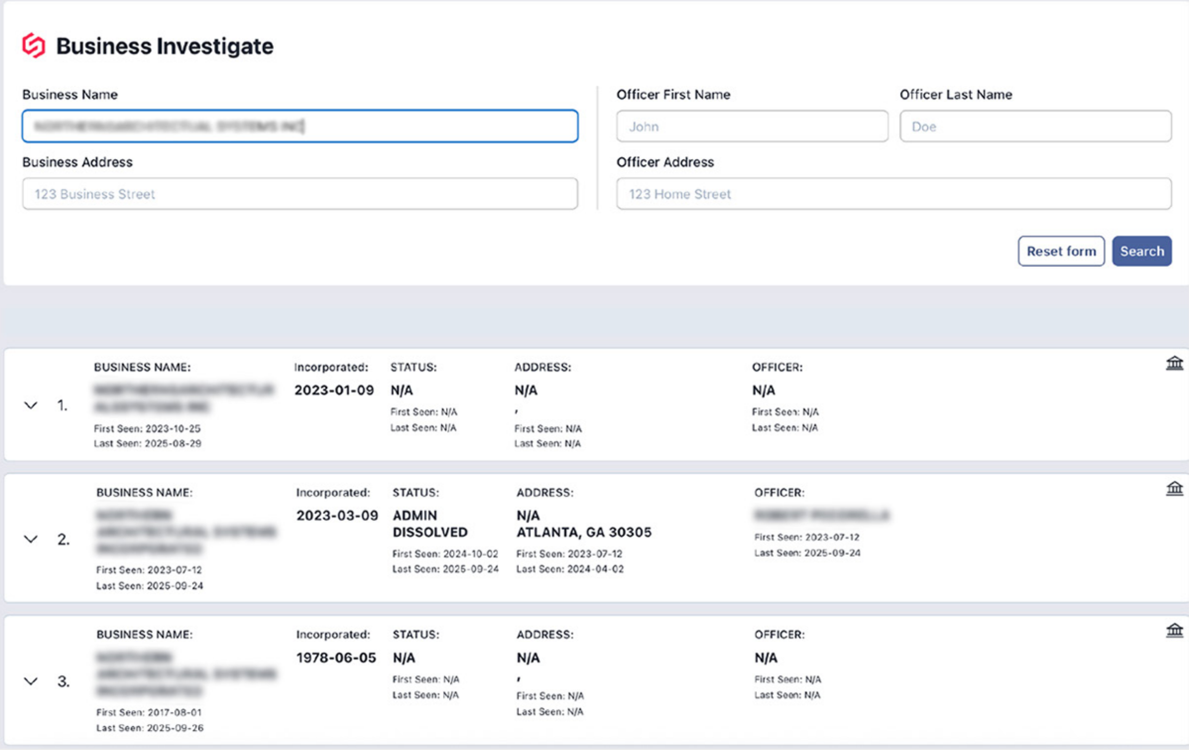
Search

UPDATE CLUSTERING

| SID | SYN \| IDT | NAME | DOB | SSN | EMAIL | PHONE | ADDRESS |
|---|---|---|---|---|---|---|---|
| VN8T | 13 \| 839 | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] |

*Screenshot from SentiLink Investigate showing an identity theft victim's information used in a suspicious application*

Further analysis of historical records in our database indicated that, in addition to entries linked to the legitimate company, the stolen identity had also been used to register a fictitious business with nearly the same name—differing only by a single added letter at the end of the first word.



Business Name: [redacted]

Officer First Name: John

Officer Last Name: Doe

Business Address: 123 Business Street

Officer Address: 123 Home Street

| | BUSINESS NAME: | Incorporated: | STATUS: | ADDRESS: | OFFICER: |
|---|---|---|---|---|---|
| 1. | [redacted]<br>First Seen: 2023-10-25<br>Last Seen: 2025-08-29 | 2023-01-09 | N/A<br>First Seen: N/A<br>Last Seen: N/A | N/A<br>,<br>First Seen: N/A<br>Last Seen: N/A | N/A<br>First Seen: N/A<br>Last Seen: N/A |
| 2. | [redacted]<br>First Seen: 2023-07-12<br>Last Seen: 2025-09-24 | 2023-03-09 | ADMIN DISSOLVED<br>First Seen: 2024-10-02<br>Last Seen: 2025-09-24 | N/A<br>ATLANTA, GA 30305<br>First Seen: 2023-07-12<br>Last Seen: 2024-04-02 | [redacted]<br>First Seen: 2023-07-12<br>Last Seen: 2025-09-24 |
| 3. | [redacted]<br>First Seen: 2017-08-01<br>Last Seen: 2025-09-26 | 1978-06-05 | N/A<br>First Seen: N/A<br>Last Seen: N/A | N/A<br>,<br>First Seen: N/A<br>Last Seen: N/A | N/A<br>First Seen: N/A<br>Last Seen: N/A |

*Screenshot of SentiLink Investigate showing the creation date of all companies with a similar name*

Our follow-up communication with the victim revealed that the criminals registered a new company using the same company name but with a single added letter, and then opened a bank account in that name. Using the fraudulent business account, they deposited five Treasury checks totaling more than $2 million and subsequently disappeared with the funds.

Another method criminals use to create bank accounts for depositing stolen checks is applying with synthetic identities. A synthetic identity may be entirely fabricated — a made-up name, date of birth, and Social Security number — or a hybrid that combines real data with fictitious or stolen elements. Fraudsters then produce supporting documentation (forged or purchased IDs, utility bills, and other records) to present to banks and fintechs when opening accounts under these synthetic identities.

A SentiLink investigation into an identity appearing in an image containing multiple checks posted in May 2025 on an online fraud market the company monitors offers an intriguing insight into this modus operandi. Each check in the image was attached to a pay stub disclosing both the company (payer) and the individual (payee) identities, along with their physical addresses.

Further analysis of the payee's information revealed that their identity was linked to two Social Security numbers: one legitimate and one fraudulent. The fraudulent SSN was associated with an email address which was associated with the payer company. Notably, while we do not have evidence that these checks have been deposited in a bank account created with this synthetic identity, SentiLink's database indicates that the personally identifiable information (PII) associated with the synthetic identity, as well as the payer company's email address, have been used in at least one suspicious loan application.

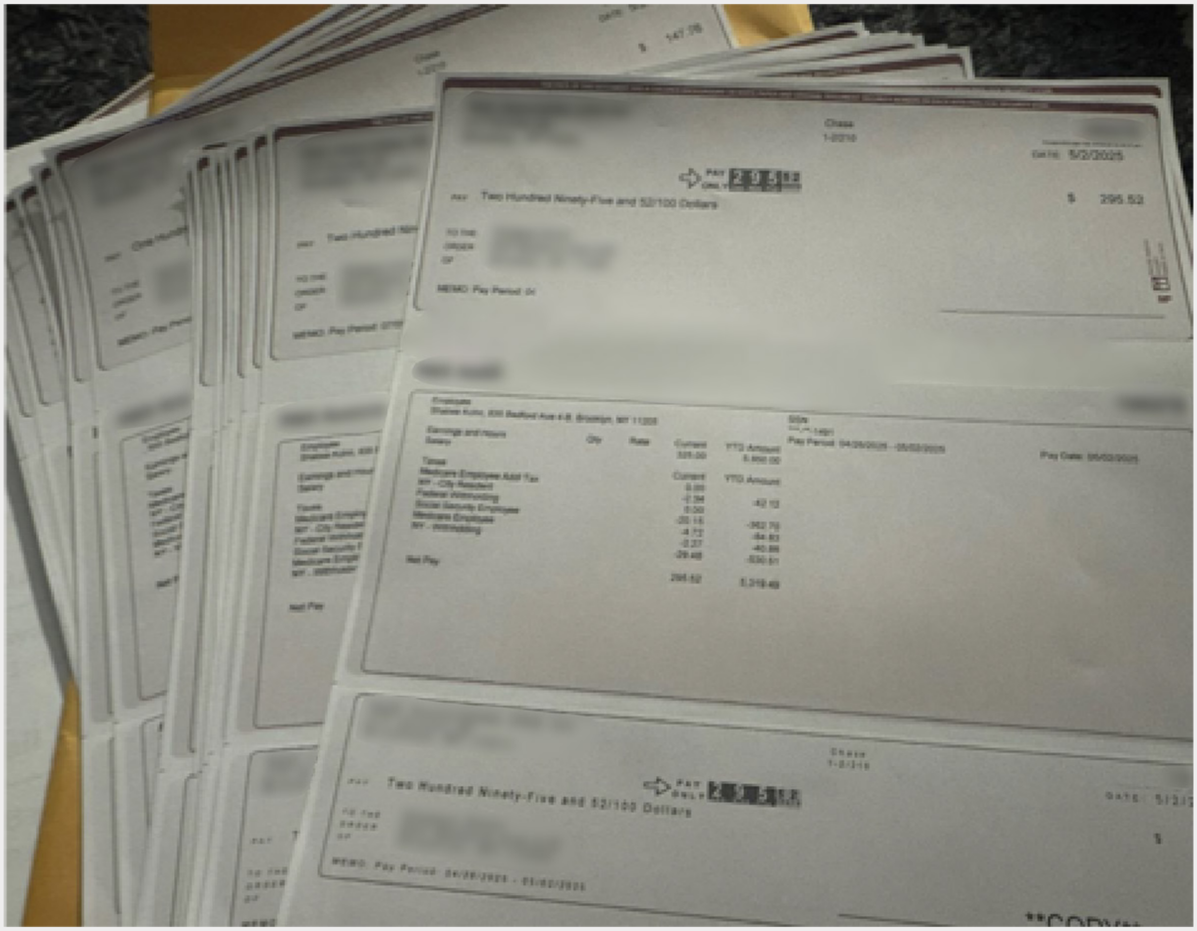
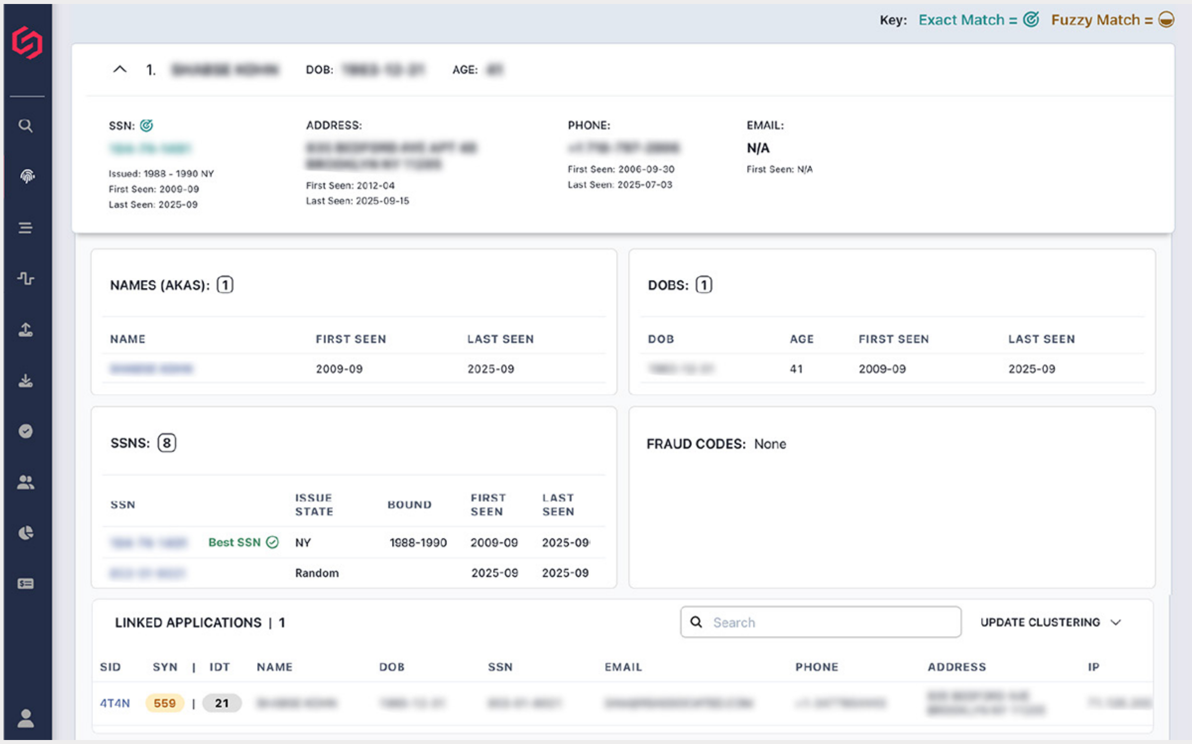

Chase
5/2/2025
Two Hundred Ninety-Five and 52/100 Dollars
$ 295.52
Two Hundred Ninety-Five and 52/100 Dollars

*Image collected during a threat intelligence effort showing stolen or fake paystubs and checks issued from a company to an individual*



1. [redacted] DOB: [redacted] AGE: [redacted]

SSN: ◎ [redacted]
Issued: 1988 - 1990 NY
First Seen: 2009-09
Last Seen: 2025-09

ADDRESS: [redacted]
First Seen: 2012-04
Last Seen: 2025-09-15

PHONE: [redacted]
First Seen: 2006-09-30
Last Seen: 2025-07-03

EMAIL: N/A
First Seen: N/A

NAMES (AKAS): 1

| NAME | FIRST SEEN | LAST SEEN |
|---|---|---|
| [redacted] | 2009-09 | 2025-09 |

DOBS: 1

| DOB | AGE | FIRST SEEN | LAST SEEN |
|---|---|---|---|
| [redacted] | 41 | 2009-09 | 2025-09 |

SSNS: 8

| SSN | | ISSUE STATE | BOUND | FIRST SEEN | LAST SEEN |
|---|---|---|---|---|---|
| [redacted] | Best SSN ✓ | NY | 1988-1990 | 2009-09 | 2025-09 |
| [redacted] | | Random | | 2025-09 | 2025-09 |

FRAUD CODES: None

LINKED APPLICATIONS | 1

| SID | SYN | IDT | NAME | DOB | SSN | EMAIL | PHONE | ADDRESS | IP |
|---|---|---|---|---|---|---|---|---|---|
| 4T4N | 559 | 21 | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] |

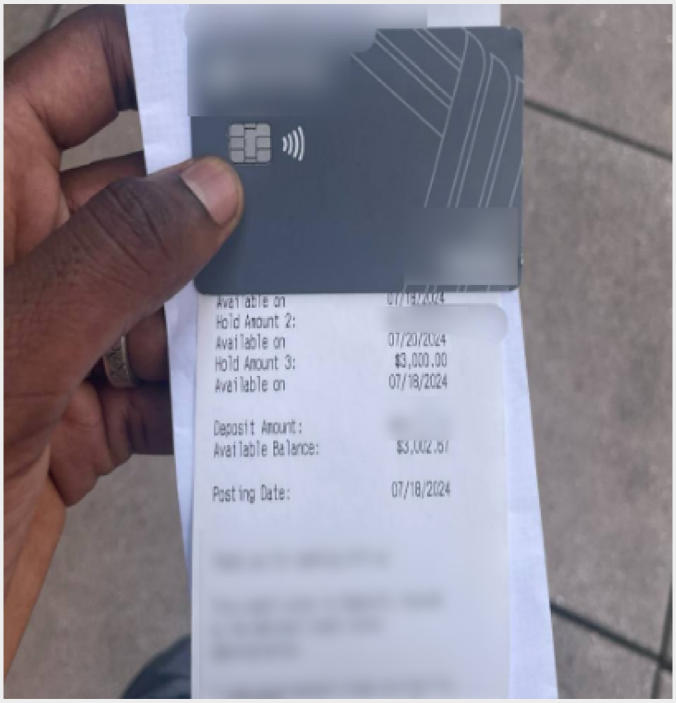
*Screenshot from SentiLink Investigate showing a synthetic identity has been used in a suspicious application*

# Legitimate account holders who collaborate with fraudsters (willingly or unwillingly)

In addition to opening bank accounts they directly control using stolen or synthetic identities, fraudsters also exploit legitimate account holders' accounts to deposit fraudulent checks. One common tactic involves issuing counterfeit or stolen checks to unsuspecting businesses or individuals as payment for goods or services. Once the payees deposit these checks, they inadvertently draw themselves and their financial institutions into the fraud scheme.

Another prevalent method relies on social engineering and relationship scams, where victims are manipulated into depositing bad checks and forwarding funds to the fraudsters. In these cases, account holders are genuine customers who become unwitting participants: they deposit what they believe are legitimate checks and then, following the scammer’s instructions, withdraw or transfer the money, only to discover later that the check was fraudulent.

Finally, some fraudsters actively seek out willing collaborators, recruiting trusted bank customers to sell access to their accounts or share in the illicit proceeds. This practice blurs the line between victim and accomplice, making detection and prevention more challenging for financial institutions.



[redacted]

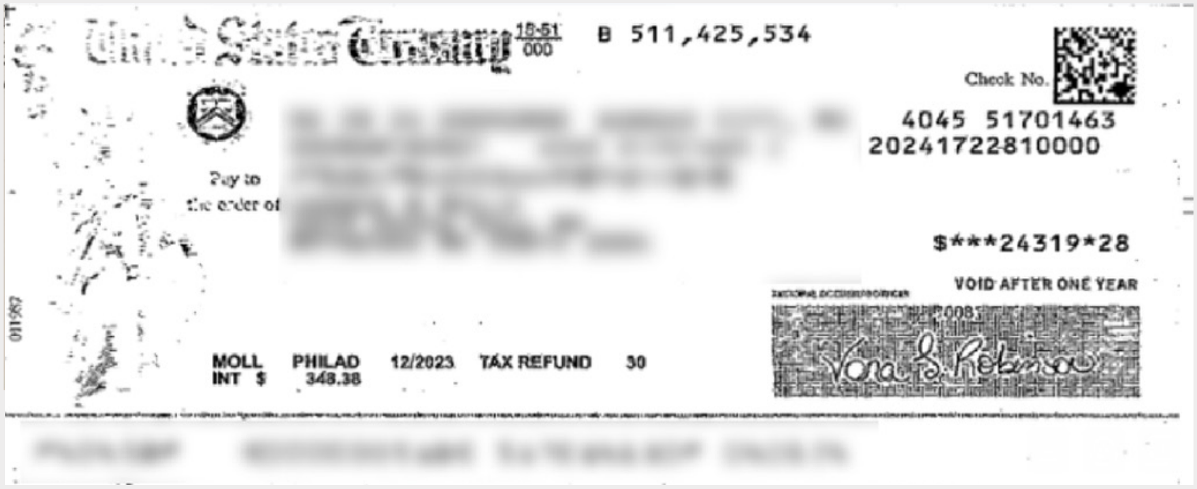
| | |
|---|---|
| Available on | 07/1[illegible]/2024 |
| Hold Amount 2: | [redacted] |
| Available on | 07/20/2024 |
| Hold Amount 3: | $3,000.00 |
| Available on | 07/18/2024 |
| Deposit Amount: | [redacted] |
| Available Balance: | $3,002.57 |
| Posting Date: | 07/18/2024 |

[redacted]

*ATM deposit slip showing the deposit of a stolen check into “J”’s bank account*

Some of the clearest evidence of fraudsters gaining access to legitimate bank accounts comes from ATM deposit slips that fraudsters post on social media — often accompanied by images of fake or stolen checks — to brag about their exploits to the online fraud community.

In one case investigated by SentiLink, a fraudster shared an ATM deposit slip over a major social media platform, boasting about the successful deposit of a counterfeit check. The investigation revealed that a fake U.S. Department of Treasury check worth more than $25,000 had been deposited into the legitimate bank account of “J”, a 21-year-old Maryland resident. While it remains unclear whether the account holder knowingly participated in the scheme or was deceived into depositing the check, this case illustrates how legitimate bank customers can become entangled in fraud, sometimes as unwitting accomplices.



United States Treasury 15-51 000 B 511,425,534

Check No. 4045 51701463 20241722810000

Pay to the order of [redacted]

$***24319*28

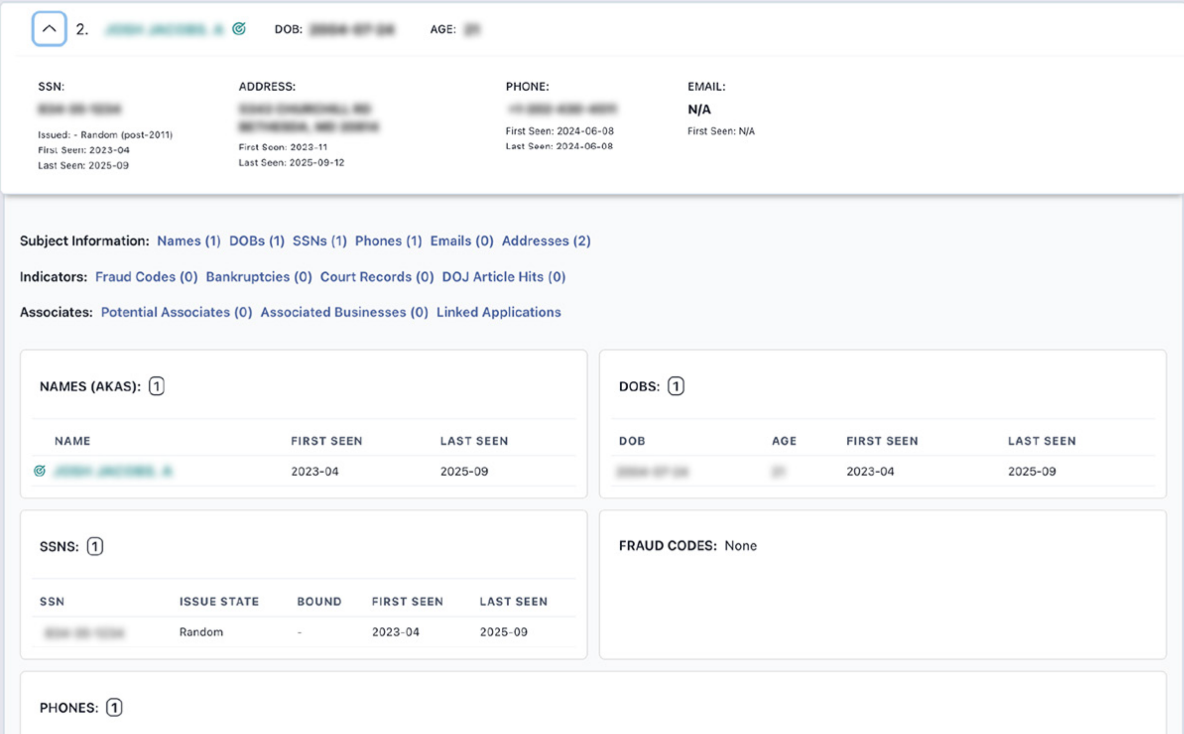
VOID AFTER ONE YEAR

MOLL INT $ | PHILAD 348.38 | 12/2023 | TAX REFUND | 30

Vona B. Robinson

[redacted]

*Counterfeit treasury check deposited into "J"'s account*



2. [redacted] DOB: [redacted] AGE: [redacted]

| SSN: | ADDRESS: | PHONE: | EMAIL: |
|---|---|---|---|
| [redacted]<br>Issued: - Random (post-2011)<br>First Seen: 2023-04<br>Last Seen: 2025-09 | [redacted]<br>First Seen: 2023-11<br>Last Seen: 2025-09-12 | [redacted]<br>First Seen: 2024-06-08<br>Last Seen: 2024-06-08 | N/A<br>First Seen: N/A |

Subject Information: Names (1) DOBs (1) SSNs (1) Phones (1) Emails (0) Addresses (2)

Indicators: Fraud Codes (0) Bankruptcies (0) Court Records (0) DOJ Article Hits (0)

Associates: Potential Associates (0) Associated Businesses (0) Linked Applications

NAMES (AKAS): 1

| NAME | FIRST SEEN | LAST SEEN |
|---|---|---|
| [redacted] | 2023-04 | 2025-09 |

DOBS: 1

| DOB | AGE | FIRST SEEN | LAST SEEN |
|---|---|---|---|
| [redacted] | [redacted] | 2023-04 | 2025-09 |

SSNS: 1

| SSN | ISSUE STATE | BOUND | FIRST SEEN | LAST SEEN |
|---|---|---|---|---|
| [redacted] | Random | - | 2023-04 | 2025-09 |

FRAUD CODES: None

PHONES: 1

*Screenshot from SentiLink Investigate Showing "J"'s information*

These findings highlight the diversity of actors embedded within the check-fraud ecosystem and underscore that the same account infrastructure can serve both organized criminal groups and exploited individuals, making detection and prevention significantly more complex.

# What does a typical sequence of account activity look like

To address the second research question, we directly engaged with fraud networks operating on encrypted messaging platforms such as Signal, WhatsApp, and Telegram. From these sources, we collected a sample of 104 stolen checks that fraudsters had posted publicly as examples to attract potential buyers. Each check displayed a visible MICR line, enabling verification and analysis.

These checks were processed by VALID Systems professionals to examine transactional behaviors, identify patterns, and trace outcomes. VALID successfully matched 95% of the fraudulent checks supplied by SentiLink, uncovering $809,089 in total fraudulent deposits linked to 64 distinct payees. More specifically, the initial sample represented 64 payees and totaled $261,058 in attempted fraud. VALID's link analysis uncovered an additional 104 fraudulent items associated with those same payees, totaling $459,000. A further 71 fraudulent items linked to different payers were found deposited into the same accounts, contributing another $89,031. In total, the $261,058 in sample fraud checks led to the identification of $809,089 in connected fraudulent deposits across multiple accounts and payers.

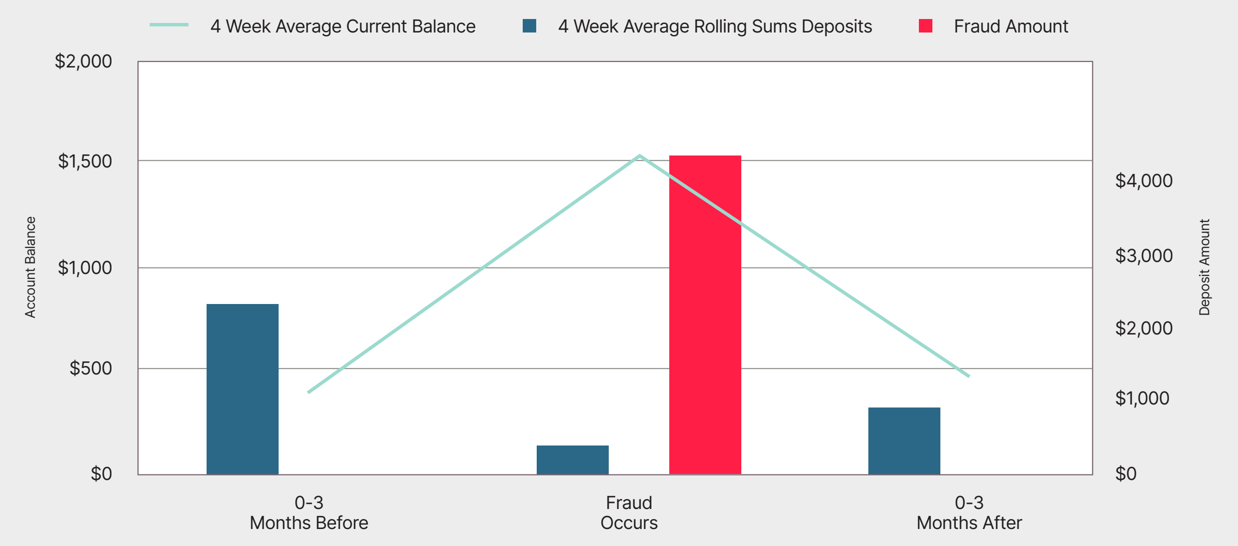
Next, we drew on VALID's segmentation of fraudulent check incidents by account age and analyzed the check data per four distinct risk profiles for account life stages:

- New Account Fraud (less than 30 days old)
- Young Account Fraud (between 2–6 months old)
- Aging Account Fraud (between 7–12 months old), and
- Tenured Account Fraud (1 year old and older)

# New account fraud (less than 30 days old)

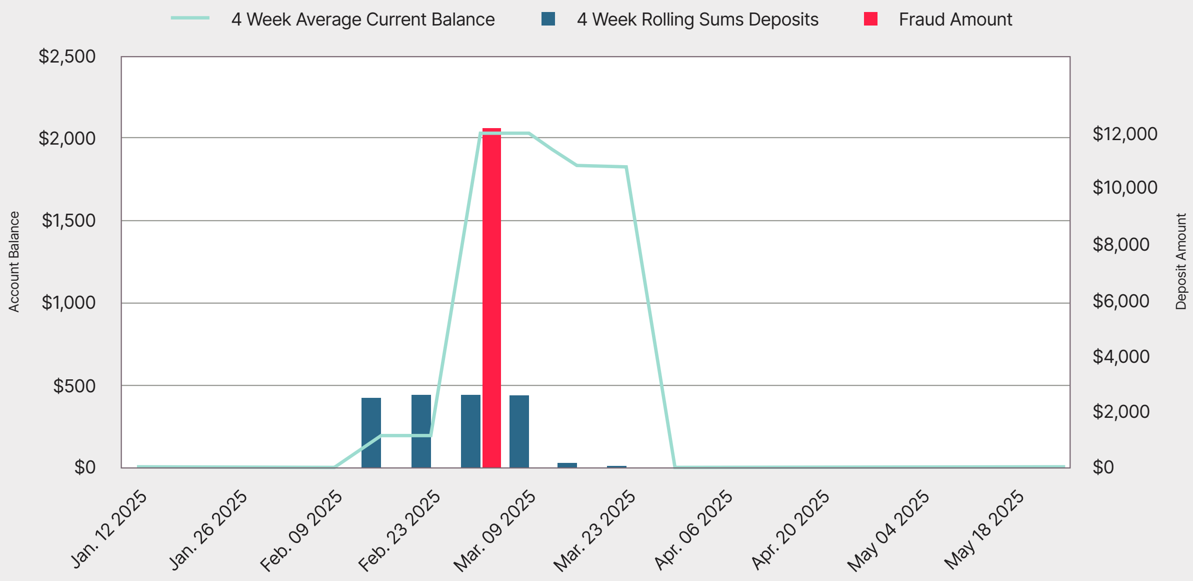
Previous analyses by VALID Systems indicate that although newly created bank accounts represent a small share of total accounts and deposited dollars, these types of accounts account for a disproportionately high volume of check-fraud activity. Specifically, VALID's study of 70 million bank accounts across seven financial institutions found that over 40% of all ATM-deposited funds in accounts less than 30 days old were fraudulent, underscoring how aggressively fraudsters target newly opened accounts. Encouragingly, detection rates in these accounts are also high, exceeding 97%.

Focusing on the dataset of checks collected from the online fraud ecosystem for this study, we found that 33% of the fraudulent checks we found on the online fraud ecosystem were deposited into newly opened bank accounts. Examination of the financial activity in these accounts prior to the fraudulent deposits revealed that the average four-week balance was approximately $1,000. On average, fraudsters made two to three legitimate deposits, each typically under $2,000, before introducing the fraudulent check. The average amount of the fraudulent deposit across our sample was $4,288, illustrating how criminals use small, legitimate transactions to "season" new accounts before executing higher-value fraud attempts.



*Average four-week balance, rolling deposit sum, and check-fraud amounts in newly-created accounts linked to stolen checks found on online fraud markets, source: Valid Systems*

In one case that stood out within this segment, the account's rolling balance remained below $200 during the first two weeks after opening. By the third week, the balance rose to approximately $2,000, followed by three consecutive legitimate deposits of about $2,600 each. Shortly thereafter, within the first month of account activity, the fraudster attempted to deposit a $12,200 fraudulent check, marking a clear escalation from low-value legitimate transactions to a high-value fraud attempt.



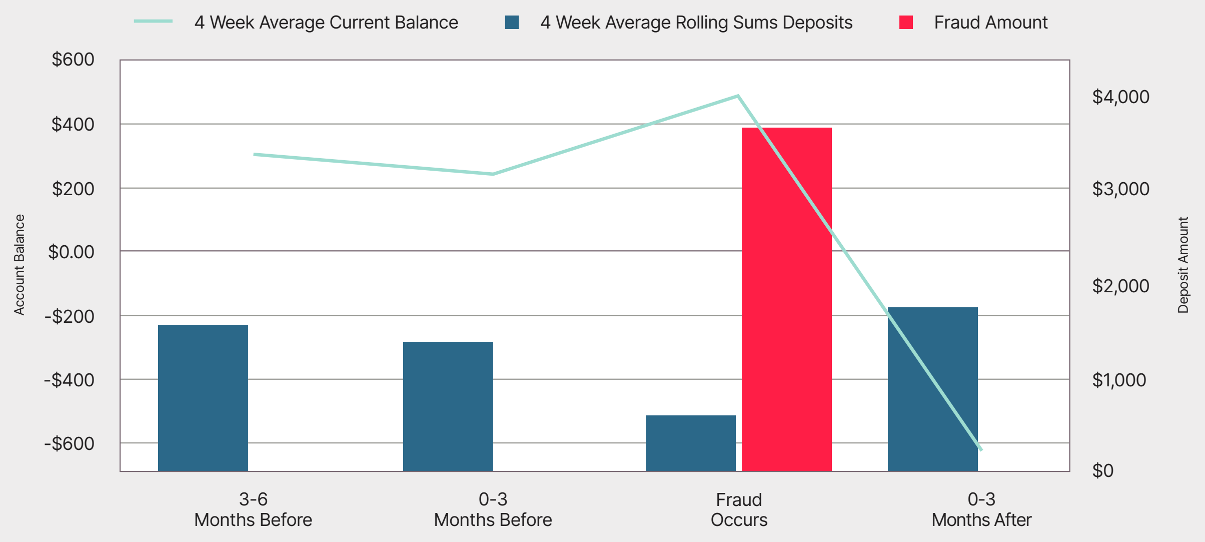
*Example of account activity: four-week balance, deposit patterns, and fraudulent check amount in a newly-opened account, source: Valid Systems*

# Young account fraud (2–6 months old)

Fraud in accounts aged two to six months is more difficult to detect and represents a more sophisticated threat. Over time, consistent legitimate deposits create a false sense of trust within the financial institution, allowing larger fraudulent transactions to slip through unnoticed.

These accounts typically maintain low balances, but fraudsters eventually exploit the established trust by making a large, anomalous deposit — often a counterfeit or stolen check. Analysis of aggregate account performance in this age range reveals this pattern clearly.

Approximately 22% of the fraudulent checks identified across the online fraud ecosystem were deposited into young accounts. On average, these accounts maintained a four-week current balance of about $300, supported by legitimate deposits averaging $1,400. In contrast, the average fraudulent check deposited into these accounts was significantly higher: around $3,635.



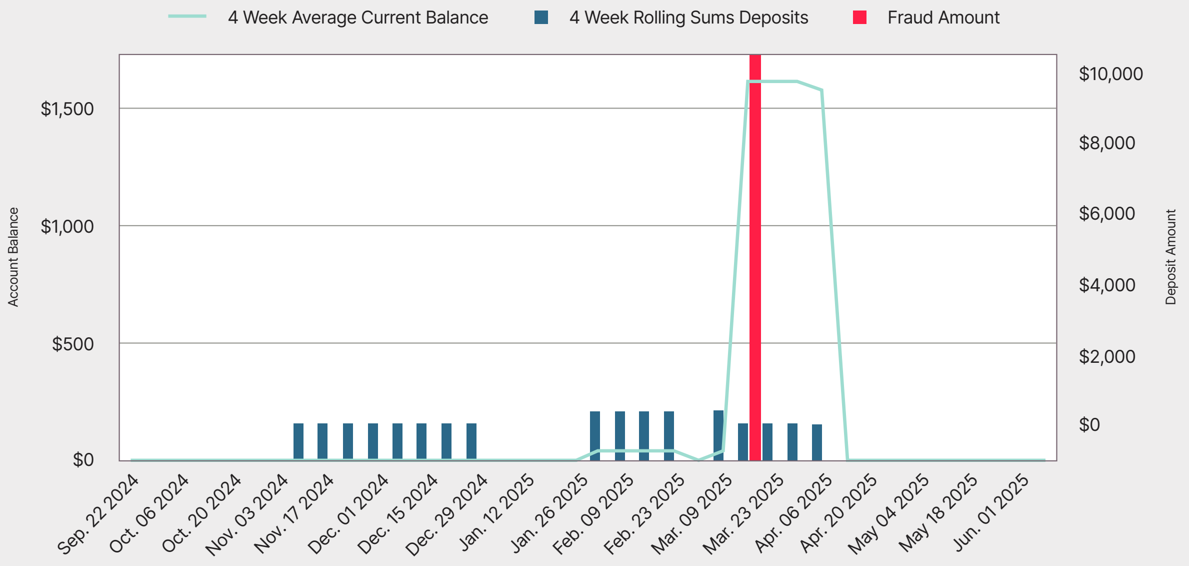
*Average four-week balance, rolling deposit sum, and check-fraud amounts in young accounts linked to stolen checks found on online fraud markets, source: Valid Systems*

A notable example of a check fraud case observed in a young account illustrates the deliberate patience and sophistication behind this type of scheme. Activity on this account began with minimal deposits — just a few dollars — over a period of a few weeks. Then the account remained largely inactive for several months. Over time, activity increased with steady weekly deposits of $389, establishing a pattern of legitimate behavior. Eventually, the account holder deposited a fraudulent check for $10,501.46, drawn on a well-known and reputable payer.

This case underscores why check fraud in these types of accounts are so difficult to detect. Fraudsters who allow accounts to "season" over time can lull banks into reducing scrutiny and relaxing risk controls, making eventual fraud harder to flag. Additionally, by stealing, altering ("washing"), or printing counterfeit checks tied to real accounts, they exploit trusted payer relationships, making detection based solely on consortium or transactional data nearly impossible.

In this instance, several factors made the fraudulent transaction particularly convincing. The payer had a nine-year history of legitimate payments, and the fraudulent check's number fell within the normal sequence of genuine payments. Moreover, good activity from this payer had been recorded across six different financial institution clients. Although the fraudulent check was three times larger than the payer's average, it was not an outlier — the largest cleared check during the same period exceeded $30,000 — further complicating detection.

Ultimately, this case highlights how fraudsters weaponize patience, blending into legitimate customer behavior before executing high-value fraud. Detecting such sophisticated schemes requires combining deposit account trend analysis with payer-level behavioral data to uncover subtle inconsistencies that signal elevated risk.



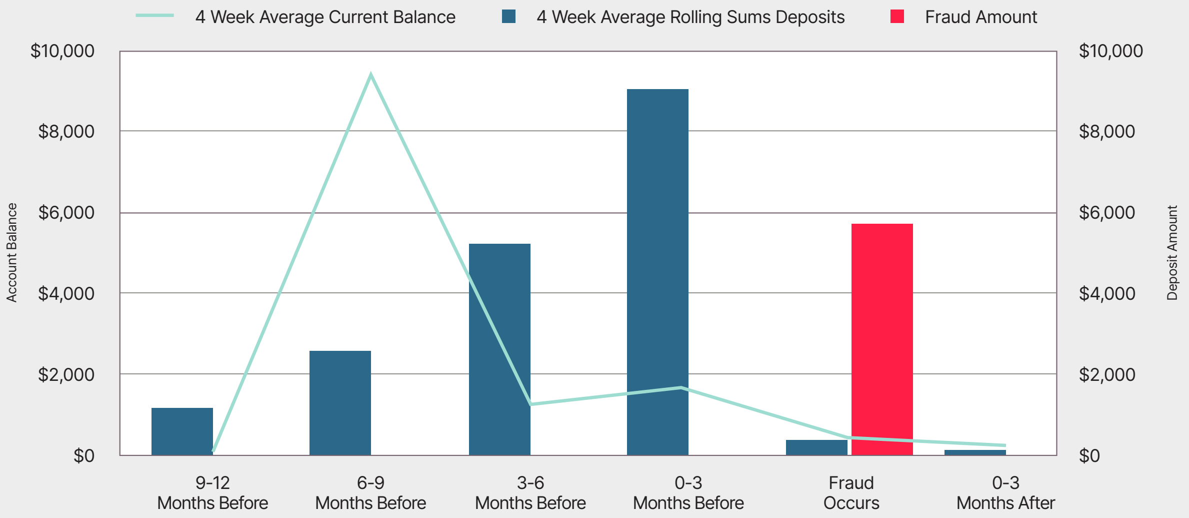
*Example of account activity: four-week balance, deposit patterns, and fraudulent check amount in a young accoun, source: Valid Systems*

# Aging account fraud (7-12 months old)

Check fraud in aging accounts often involves legitimate customers with consistent account activity who suddenly appear to “go bad.” In this segment, primary checking customers typically use their accounts as expected, maintaining low balances and demonstrating stable transactional patterns, until they either fall victim to a scam or willingly collaborate with a fraudster in hopes of making quick money. While some cases still involve fraudsters opening accounts themselves and waiting for the right moment to strike, it has become increasingly common for fraudsters to conspire with existing, legitimate account holders to carry out the fraud. This evolution represents a shift from sleeper accounts created by criminals to the exploitation or recruitment of trusted customers.

Our analysis found that 7% of the fraudulent checks we collected from the online fraud ecosystem for this research were deposited into aging accounts. Prior to the fraud event, these accounts held an average four-week balance of about $1,300. Consistent and gradually increasing legitimate deposits averaging $2,500 were observed leading up to the fraudulent activity. In contrast, the average fraudulent check deposited into these accounts was significantly higher, at approximately $5,746.

This pattern underscores how fraudsters leverage established trust and consistent account behavior to bypass detection, turning ordinary customer accounts into vehicles for check fraud.

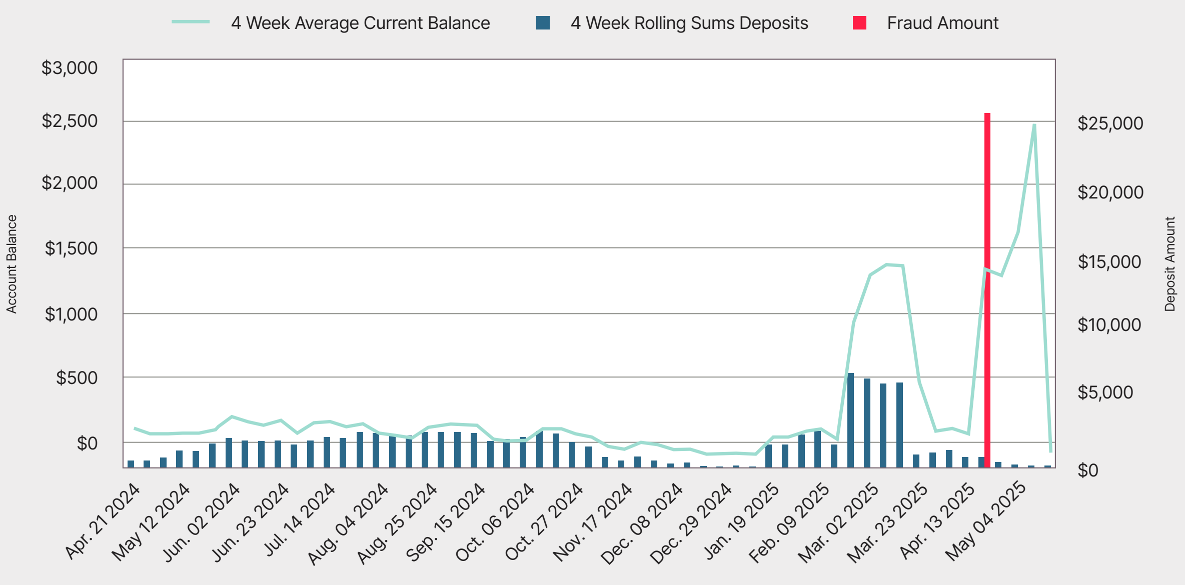


*Average four-week balance, rolling deposit sum, and check fraud amounts in aging accounts linked to stolen checks found on online fraud markets, source: Valid Systems*

In one illustrative case of an aging account scam, the account consistently carried a negative balance and maintained a low average balance from opening. For the first ten months, deposits never exceeded $2,600, and funds were typically spent almost immediately after posting, reflecting the normal behavior of a cash-strapped but otherwise legitimate account.

Then, just as the account reached its one-year mark, the pattern shifted dramatically. Several deposits exceeding $6,000 were made in quick succession, followed by the deposit of a fraudulent check for $25,680. This sudden change in behavior after months of predictable activity fits a common pattern in aging account fraud, where fraudsters exploit accounts that appear stable and low-risk to financial institutions.

Notably, the payer associated with this fraudulent check appeared carefully selected, displaying characteristics designed to evade detection. The payer was a medium-sized business with activity observed across three financial institutions, an average cleared check amount of over $33,000, and a fraudulent check sequence number that fell neatly within the range of legitimate items. These factors combined to make the fraudulent transaction appear routine and credible, complicating efforts to identify it as suspicious.

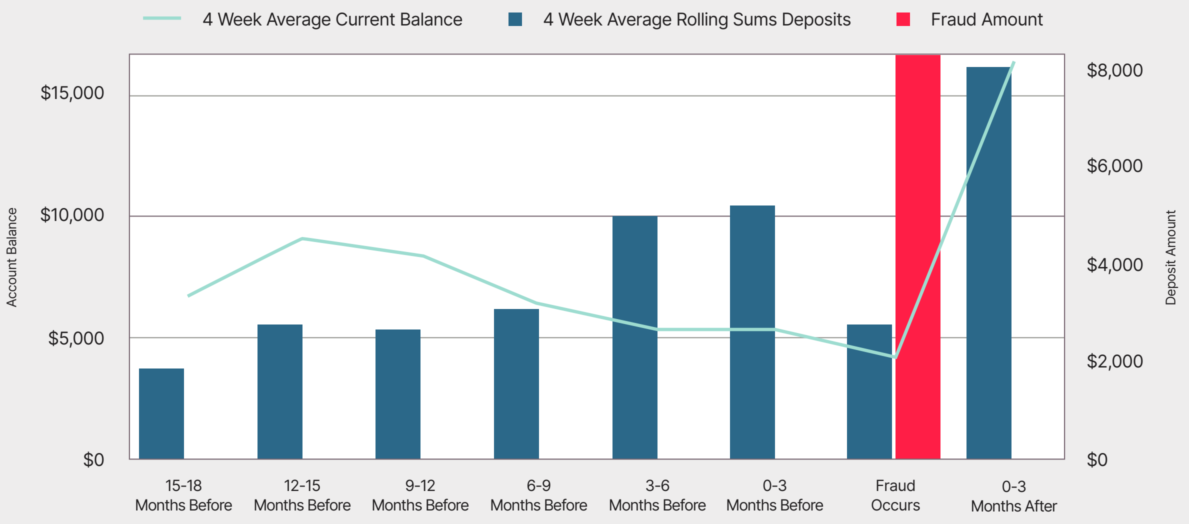


*Example of account activity: four-week balance, deposit patterns, and fraudulent check amount in aging account, source: Valid Systems*

# Tenured account fraud (1 year and older)

Tenured accounts — those open for more than one year — represent the majority of all accounts and deposit activity. They also include the largest proportion of legitimate customers who become entangled in fraud schemes involving counterfeit or stolen checks. This segment exhibits the most complex forms of check fraud, as it encompasses a range of scenarios: customers unknowingly aiding fraudsters, willingly collaborating with them, being deceived into sending money to scammers, or experiencing full account takeovers. For financial institutions, detecting fraud in these accounts is particularly challenging, especially when the customer is the victim of a scam or unknowingly deposits a fraudulent check as part of a legitimate-looking transaction.

In our dataset, 37% of the fraudulent checks collected from the online fraud ecosystem were deposited into tenured accounts. The average four-week balance in these accounts exceeded $5,000, significantly higher than in any other account type. These accounts also displayed regular, legitimate deposits, typically greater than $2,500 per month. The average value of a fraudulent check deposited in this segment was $8,277, highlighting the elevated financial stakes and the heightened risk of losses when long-standing, trusted accounts are exploited.

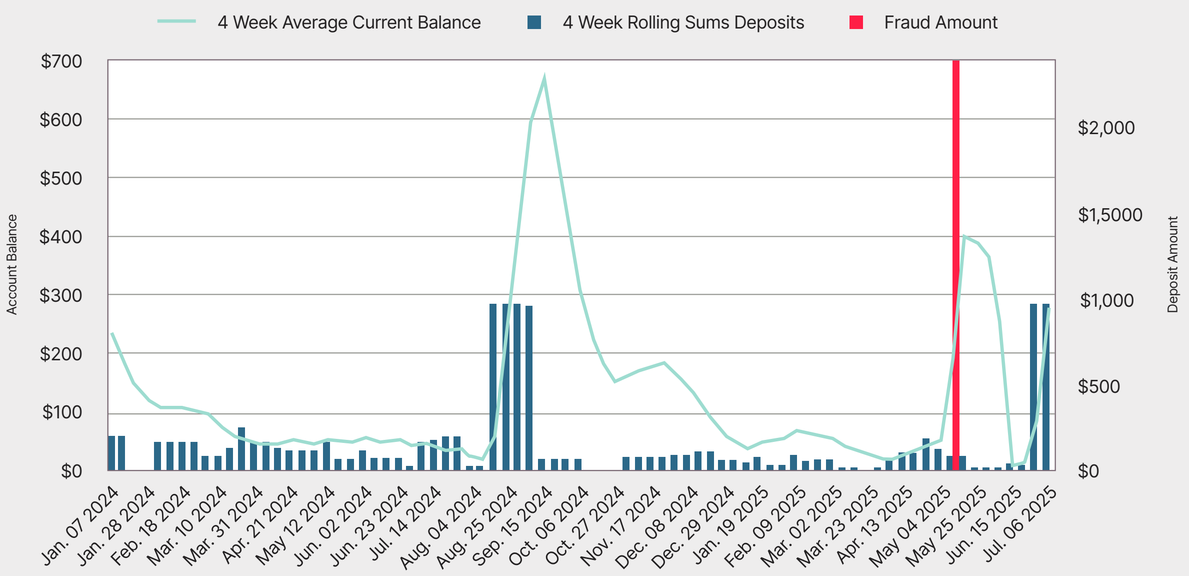


*Average four-week balance, rolling deposit sum, and check-fraud amounts intenured accounts linked to stolen checks found on online fraud markets, source: Valid Systems*

One of the accounts where a fraudulent check was deposited was just under two years old. The account showed a history of smaller deposits and steady daily activity, consistent with legitimate use. However, the fraudulent check for $2,400 was more than twice the size of any previous deposit made by the account holder.

The financial institution, leveraging VALID alerts, correctly identified the transaction as suspicious, flagged the deposit, and withheld the funds. As a result, the bank prevented any financial loss. In the weeks that followed, the customer resumed normal deposit behavior, and the institution successfully retained the relationship without consequence.

This case exemplifies a classic scam scenario in which the legitimate account holder was deceived by a fraudster into depositing a fraudulent check without any intent to defraud the bank. It highlights the importance of early detection and balanced risk management practices that protect both financial institutions and their customers.



*Example of account activity: four-week balance, deposit patterns, and fraudulent check amount in tenured account, source: Valid Systems*

Interestingly, during this same period, additional fraud attempts were observed involving the same payer whose check had been altered and deposited in the earlier example. Although this payer is relatively small, they have a seven-year history of legitimate payments with deposit activity across four different financial institutions.

Fraud was attempted at two of these institutions, on both newly opened and long-standing (tenured) accounts. The most tenured account holder to deposit a fraudulent check from this payer had maintained their account for 20 years, displaying a profile nearly identical to that of the two-year-old account discussed earlier: long, consistent activity characterized by smaller deposits and low, fluctuating balances.

In this case, a fraudulent check for $2,500 was deposited, followed shortly by legitimate deposits, further complicating detection. This pattern underscores how fraudsters exploit even well-established, trusted relationships between payers and account holders to disguise illicit activity within normal transactional behavior.

# Conclusions

The evolution of check theft and check fraud in the United States since 2021 represents a fundamental transformation in financial crime. What began as opportunistic mail theft and basic “check washing” has matured into a coordinated, technology-enabled ecosystem connecting identity theft, synthetic identity creation, and account manipulation.

Our findings demonstrate that fraudulent check deposits now occur across all stages of account maturity from newly opened to long-tenured accounts, and that both synthetic identities and legitimate account holders play central roles in enabling the crime. In newly opened accounts, fraudsters rely on stolen or fabricated identities to create short-lived “burner” accounts for quick cash-out. In contrast, fraud in aging and tenured accounts increasingly involves real customers — some deceived, others complicit — whose transactional histories lend legitimacy to illicit deposits.

The data also highlight a troubling dynamic: while new-account fraud is typically easier to detect, fraud in older, established accounts is more sophisticated, more damaging, and harder to identify. By mimicking normal customer behavior, maintaining consistent deposits, and exploiting trusted payer relationships, fraudsters exploit gaps in traditional risk models.

Ultimately, check fraud today is no longer an isolated financial crime; it is part of a broader fraud supply chain that spans digital identity fabrication, account brokering, and social engineering. Breaking this chain requires coordinated intervention, greater data transparency across institutions, and modernization of fraud detection systems.

This complexity demands an equally sophisticated defense. Static controls and one-size-fits-all fraud strategies leave institutions vulnerable to targeted exploitation. Financial institutions must instead adopt dynamic, multi-layered detection frameworks that combine identity intelligence, behavioral analytics, and real-time transaction monitoring to adapt alongside fraudsters.

Equally critical is collaboration. By leveraging a network of data, linking behaviors across financial institutions, and sharing intelligence on emerging threats, banks can better anticipate coordinated fraud activity and mitigate risk industry-wide. The partnership between VALID and SentiLink demonstrates the power of data-driven insights to expose hidden patterns, strengthen detection strategies, and protect both financial institutions and their customers.

Check fraud is no longer a legacy crime. It has become a dynamic, data-driven enterprise leveraging technology, social engineering, and systemic blind spots. The findings in this report make clear that both prevention and detection must evolve accordingly. Financial institutions that integrate behavioral analytics, cross-industry data collaboration, and proactive customer engagement will be best positioned to reduce losses and protect consumers from the widening reach of organized financial fraud.

The fraud landscape will continue to evolve. With the right tools, partnerships, and intelligence, financial institutions can stay ahead of the attackers rather than chasing them from behind.

SentiLink