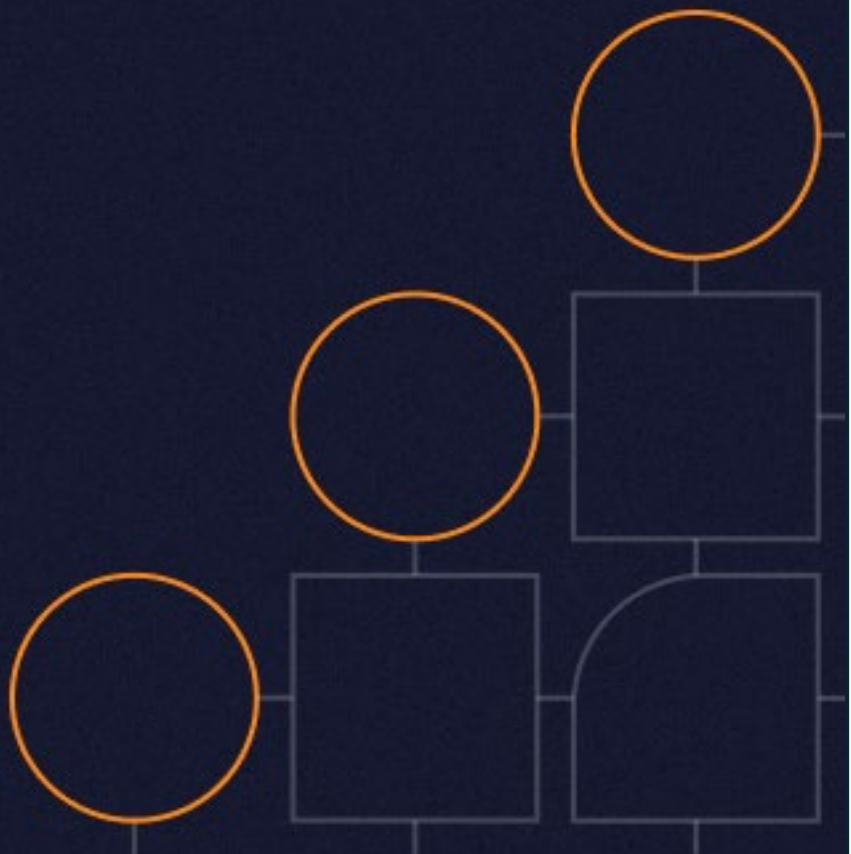
VALID systems

Sleeper Accounts, Synthetic Identities, and Stolen Checks: A Guide to Modern Check Fraud



Executive Summary

Check deposit fraud has evolved into a **highly organized, multi-faceted threat**, leveraging everything from synthetic identities to compromised legitimate accounts. In collaboration with SentiLink, a leader in synthetic identity detection, VALID conducted a joint investigation to better understand how fraudsters operate and how their schemes move through the financial ecosystem.

This research underscores the **critical importance of real-time detection as well as customer behavior** and offers insights into evolving fraud tactics that can inform stronger, more adaptive defenses for financial institutions. Across multiple fraud types and analysis into account age segments, several high-level insights emerged from the study:

- **Fraud is Organized and Widespread:** Check fraud is occurring at **every institution** analyzed, indicating industry-wide exposure. Fraud rings coordinate activity across multiple banks and accounts. New accounts are especially targeted by organized schemes – in some cases, **nearly half of the deposit dollar value in new accounts turned out to be fraudulent**. This points to a **concerted, organized attack on banks' account onboarding and deposit processes**.
- **Tactics Evolve Over the Customer Lifecycle:** The nature of fraud changes as an account ages. **Early-stage accounts** face **"fast hit" attacks** (often using synthetic or stolen identities to open and cash out quickly). **Mid-stage accounts** may serve as **"sleeper cells"**, where fraudsters invest time to establish normal behavior before a big theft. **Late-stage (aged) accounts** often involve **social engineering, account takeovers, or collusion with legitimate accountholders**. In other words, fraudsters continuously adapt their methods – from identity-based fraud at onboarding to social exploitation of trusted customers – exploiting whatever weakness is present at each phase of the account's life cycle.
- **Detection Effectiveness Declines with Account Age:** Our findings show that while banks are highly effective at catching fraud in new accounts (about **97% detection rate** in the first month), their success rate drops for older accounts (**falling to ~87% for accounts over one year old**). This decline is due to the increased sophistication of attacks on seasoned accounts and the challenge of discerning malicious behavior from genuine long-term customer activity. More fraud in older accounts slips through initial screening, which means **fraud losses concentrate in the later stages** if not addressed with advanced monitoring.
- **High-Risk Windows Require Targeted Strategies:** There is no single silver bullet for check fraud. **Different account ages present different risk "windows" and attack patterns**, meaning a static fraud prevention strategy will leave gaps. Financial institutions must adopt a **multi-layered, dynamic approach** that considers account tenure and behavior. By tailoring detection tools to these fraud typologies and behaviors, banks can more effectively shut down fraud at every stage while minimizing impact to genuine customers.

Data Study Background

SentiLink researchers engaged directly with fraud networks on encrypted messaging platforms like **Signal** and **Telegram**, where fraudsters openly advertised their ability to bypass financial institutions' defenses. To establish credibility, fraudsters provided **sample checks**, claiming they could be deposited without detection. Leveraging VALID's network, which processes **over $4 trillion in annual check volume**, we tracked these checks across financial institutions to analyze behaviors, patterns, and outcomes. The **7 financial institutions** analyzed represent **over 70M unique accounts with $200B deposited across Mobile, ATM, and Branch channels**. This study goes beyond the fraudulent check item to analyze the behavior of each impacted account, detailing performance before, during, and after the fraud check is deposited.

The results were striking: **VALID successfully matched 95% of the fraudulent checks** provided by SentiLink, uncovering **$809,089 in total fraudulent deposits** tied to 64 distinct payees. Our analysis revealed how fraudsters exploit **both good-standing and synthetic accounts**, exposing financial institutions to significant risk across multiple attack vectors.

Initial Observations from the VALID + SentiLink Analysis

- **95%** of the **75 fraudulent items** provided by SentiLink were matched within VALID's network.
- Fraud check samples represented **64 distinct payees**, totaling **$261,058** in attempted fraud.
- An **additional 104 fraudulent items** from the same payees were uncovered, totaling **$459,000**.
- Another **71 fraudulent items** linked to **different payers** were deposited into the same accounts, adding **$89,031**.
- From the **initial $261,058** of fraud sample checks, VALID identified **$809,089 in total fraudulent deposits through link analysis** when identifying all fraud activity from additional payers and accounts

The propensity and characteristics of check fraud change markedly as an account matures. Our analysis segmented fraudulent check incidents by the age of the deposit account, revealing **distinct high-risk patterns** at each stage of an account's life:

- New Account Fraud (< 30 Days)
- Young Account Fraud (2 – 6 Months)
- Aging Account Fraud (7 – 12 Months)
- Tenured Account Fraud (> 1 Year)

Check Deposit Fraud Patterns Observed

Check fraud is not a **one-size-fits-all** problem — it spans multiple attack strategies, each requiring different detection and response techniques. By tracing fraudulent checks through the deposit ecosystem and analyzing account behaviors, we identified several recurring patterns:

- **First-Party Fraud – Real IDs, Bad Checks**
  Fraudsters open accounts with authentic credentials but deposit counterfeit or stolen checks.
- **Synthetic Fraud**
  Using fabricated or synthetic identities, criminals create new accounts that appear genuine on paper, then deposit fraudulent checks. These synthetic accounts often pass initial identity verification checks, making them a potent tool for new account fraud.
- **Scammer-Driven Fraud**
  Fraudsters issue fraudulent checks to unsuspecting businesses or individuals as payment for goods or services (for example, overpaying with a fake check and asking for a refund of the difference). The payees deposit the checks, unknowingly pulling themselves and their banks into the fraud scheme.
- **Romance & Victim Scams**
  Through social engineering and relationship scams, victims are manipulated into depositing bad checks and sending funds to the fraudsters. The account holders in these cases are legitimate customers who become unwitting participants – they deposit a check (often believing they received legitimate funds) and later withdraw or transfer money at the scammer's direction, only to have the check bounce.
- **Good Gone Bad**
  Long-standing, trusted customers either sell account access, are socially engineered into writing fraudulent checks, or collude directly with fraudsters to share proceeds.

By following the path of these checks — from origination to deposit — and analyzing **balances, deposit timing, and account behaviors**, we uncovered actionable insights into fraudster behaviors that help inform more precise detection strategies.

New Account Fraud (Accounts < 30 Days Old)

New account fraud metrics:

- Total percentage of check deposit dollars: 4.4%
- Total percentage of check deposit charge off dollars: 14.0%
- Fraud deposit rate: 2.53%
- Fraud detection rate: 97.4%

While the percentage of accounts and total dollars deposited by new accounts is small, the attack volume is significant. Across all FI's analyzed, **over 40% of all ATM deposited dollars** in accounts under 30 days old were fraudulent, highlighting how aggressively fraudsters target newly opened accounts.

Additional insights for this segment:

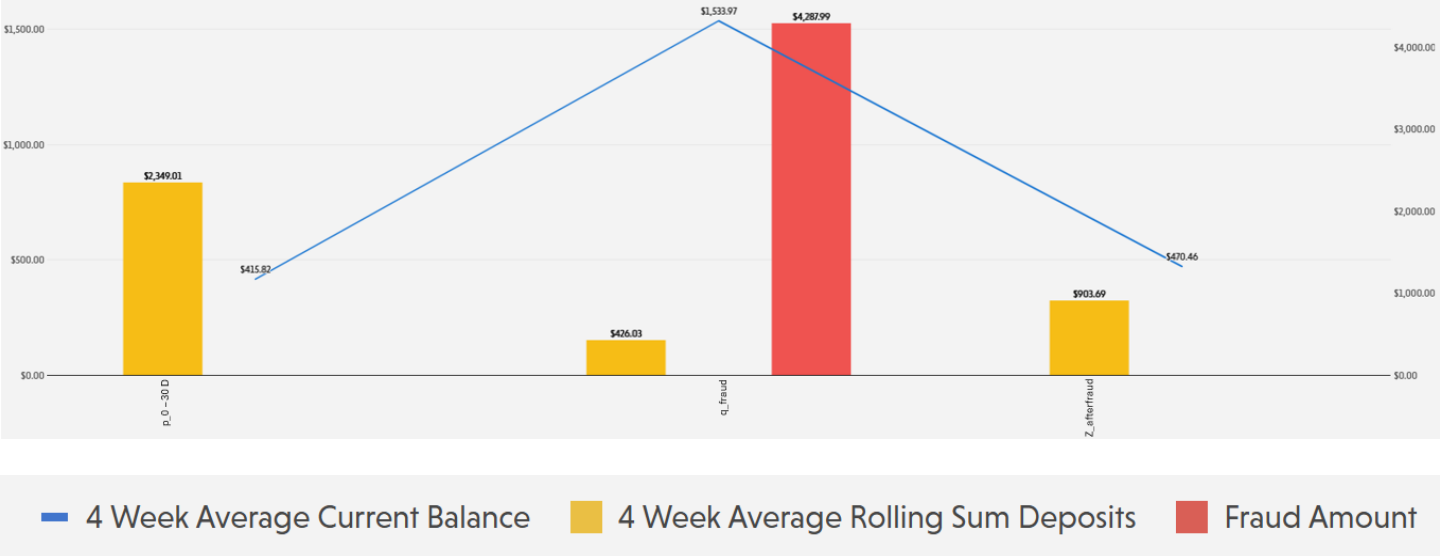
- The **average check size** is **$7,609**, more than **2x higher** than other age segments (<$3,000).
- This increase is partly driven by legitimate balance transfers, but **large-dollar fraud attempts** are the primary driver.
- Behavioral patterns are remarkably consistent:
    - Fraudsters make **several smaller, legitimate deposits** first.
    - A **large fraudulent check** is then introduced, often **2x larger** than the largest prior good deposit.
- On average, **first-party fraud in new accounts involves a single fraudulent check attempt**.

Below is the aggregated performance in Figure #1 of a fraud account < 30 days old that presents a fraudulent check for deposit then later is closed and charged off by the FI.

New Account Fraud (< 30 Days Old)

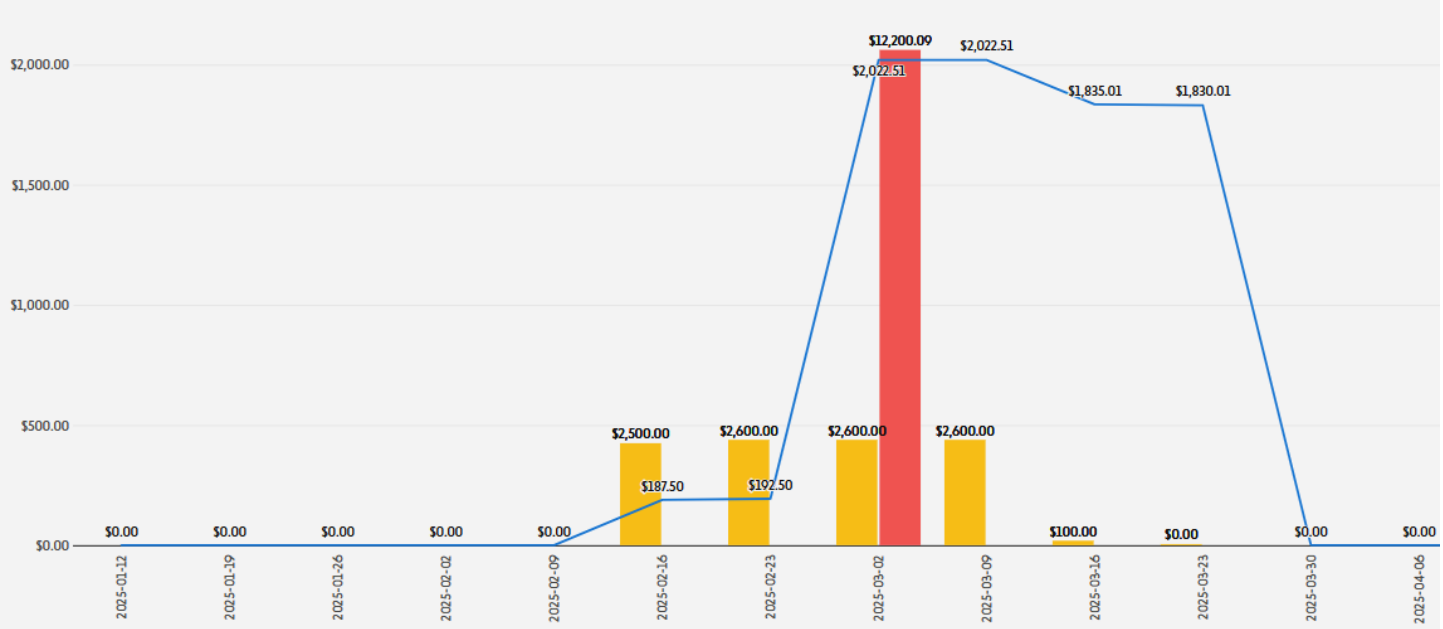
- *Average 4-week current balance around $1,000*
- *Fraudster often makes 2 – 3 good deposits of ~$2,000*
- *Average fraudulent check deposited is $4,288*

Figure #1



In one example (Figure #2), an account showed **three consistent $2,600 deposits**, followed by a **$12,200 fraudulent check** attempt within the first month of account opening.

Figure #2



Young Account Fraud (2–6 Months Old)

Young account fraud metrics:

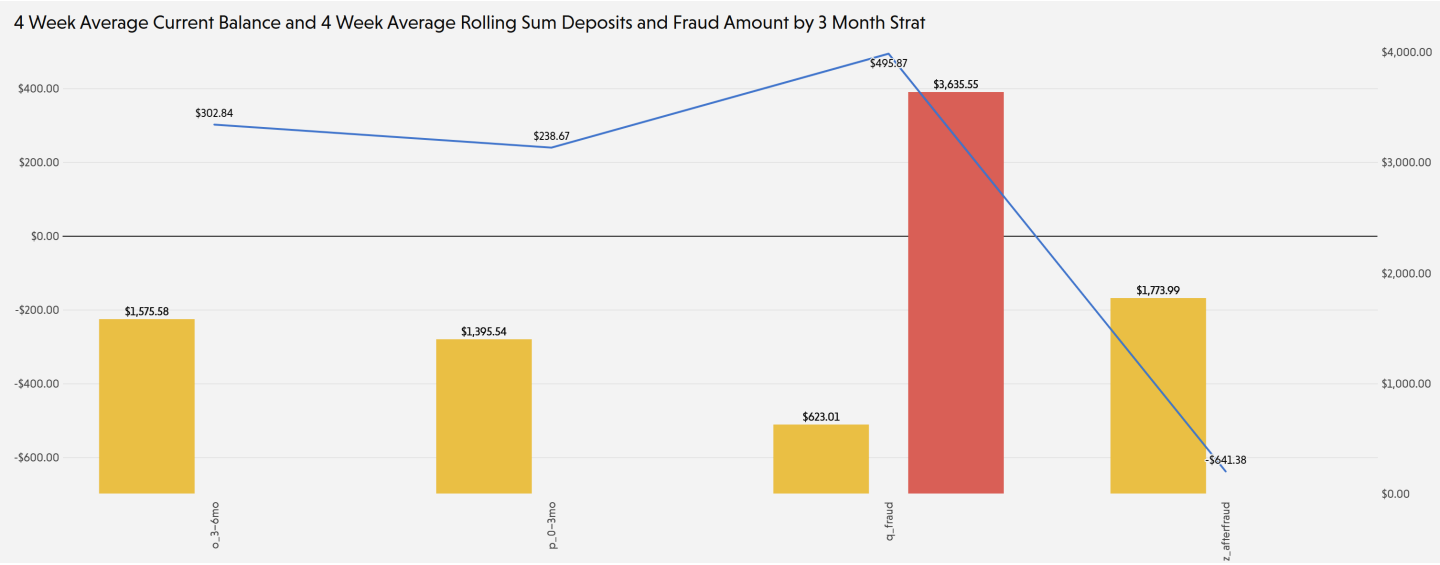
- Total percentage of check deposit dollars: 3.1%
- Total percentage of check deposit charge off dollars: 35.2%
- Fraud deposit rate: 3.27% (highest among any account age group)
- Fraud detection rate: 92.6%

Fraud in accounts aged **2–6 months** is **harder to detect** and represents a **more sophisticated threat**. Consistent, legitimate deposits over several months build **false confidence** by the financial institution and allow for more fraud to get through. Accounts maintain **low balances**, but fraudsters eventually attempt a **large, anomalous deposit** of a fraudulent check as seen in the aggregate performance of accounts 2 – 6 months old.

Young Account Fraud (2 – 6 Months Old)

- *Average 4-week current balance around $300*
- *More consistent, good deposits made on average of $1,400*
- *Average fraudulent check deposited is $3,635*

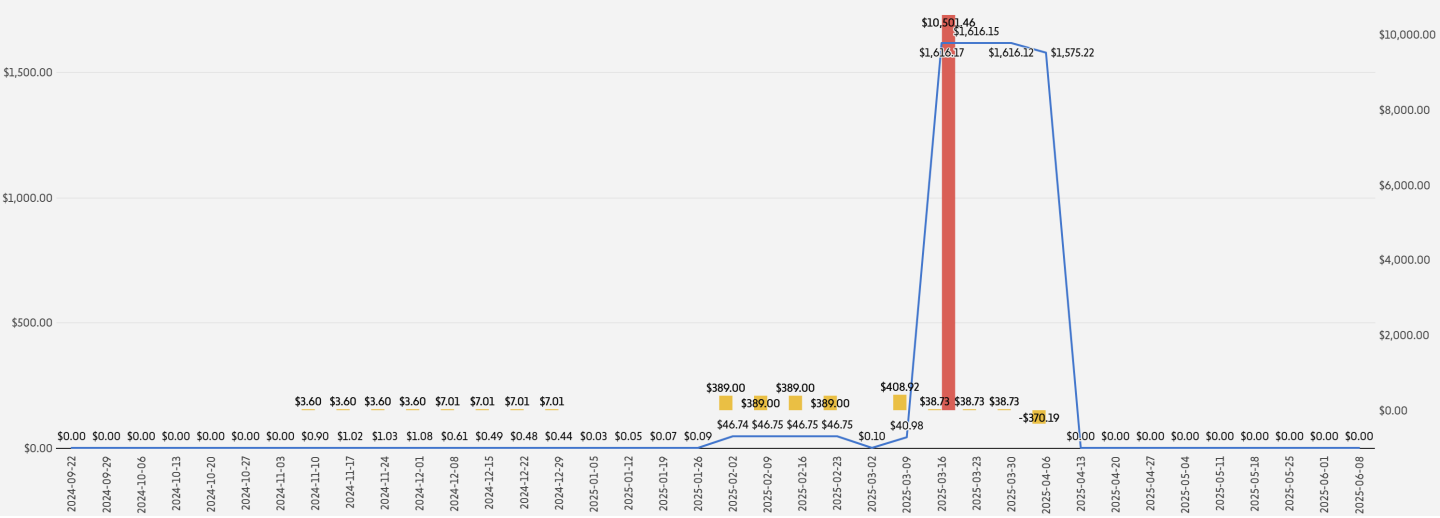
Figure #3



A notable example of a sleeper fraud account, (Figure #4) illustrates the fraudsters strategy:

- The account started with **minimal deposits** of just a few dollars.
- After months of low activity, the customer shifted to **steady weekly deposits** of **$389**.
- Finally, the account deposited a **$10,501.46 fraudulent check**, drawn on a reputable payer.

Figure #4



What makes this type of fraud so complicated is twofold:

1. Fraudsters who patiently lie in wait for banks to relax risk settings and scrutiny on aged accounts can be richly rewarded
2. Either stealing, washing, or fraudulently printing checks on the right account can make detection based on consortium data nearly impossible

In this scenario, the fraudster had multiple things going for them based on the very large payer's previous history:

- Payer has a 9-year history of payments, with the fraud check within check sequence number of good payments
- Good activity from this payer has been identified across 6 different FI clients
- While the check was **3x larger than the payer's average**, it was not an outlier as the largest cleared item during the same timeframe had been for over $30K — making detection far more challenging.

These findings highlight how **fraudsters weaponize patience**, blending into normal customer patterns before striking with significant, high-value fraudulent activity. Pairing **deposit account trends with payer data and behavior** are required to identify these types of more patient, sophisticated deposit fraud.

Aging Account Fraud (Accounts 7 – 12 Months Old)

Aging account fraud metrics:

- Total percentage of check deposit dollars: 3.7%
- Total percentage of check deposit charge off dollars: 15.4%
- Fraud deposit rate: 0.87%
- Fraud detection rate: 89.9% (first segment that sees > 10% of fraud attempted get through)

Here in this segment, we start to see more good customers with consistent activity going bad. This is where primary checking customers are using their accounts as expected, maintain low balances, and are either scammed themselves by the fraudster or

partner with the fraudster to make some quick money. There are cases still where fraudsters open the account and wait to strike, but it is now more common that fraudsters are conspiring with a good account holders to perpetrate the fraud.

Aging Account Fraud (7 – 12 Months Old)

- *Outside of one anomalous account, average 4-week current balance around $1,300 prior to fraud event*
- *Consistent, larger good deposits made on average of $2,500 and increasing over time*
- *Average fraudulent check deposited is $5,746*

Figure #5

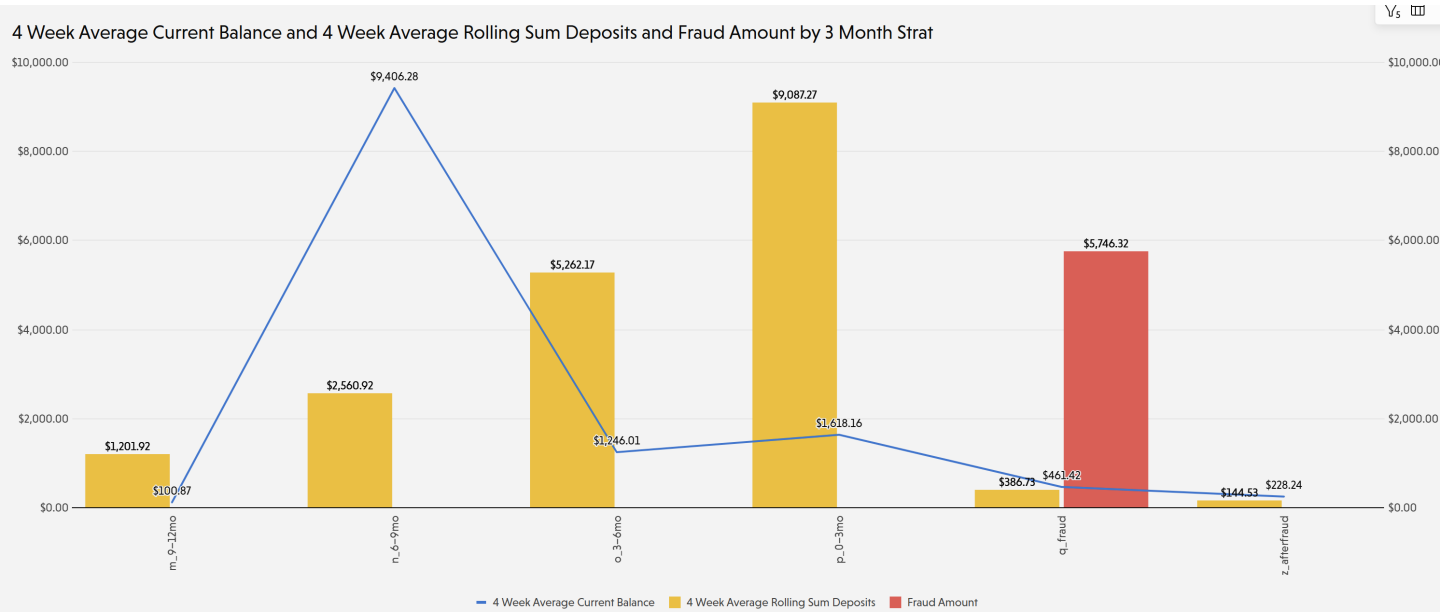
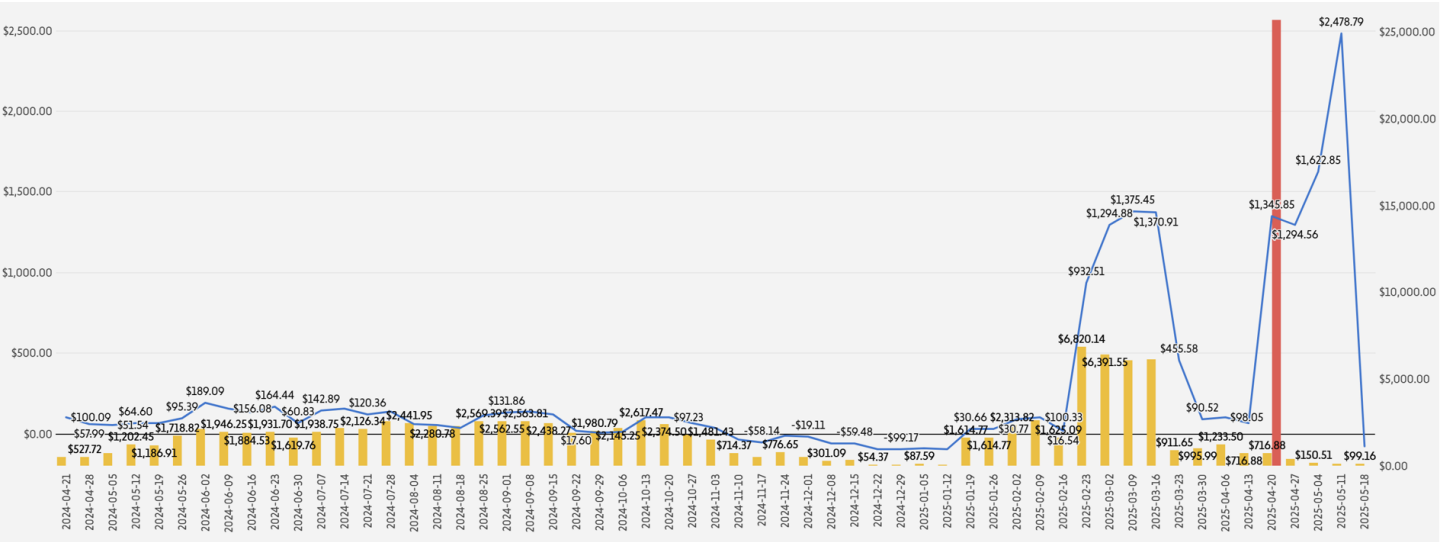


Figure #6 is a great example of the common aging account scam. The account consistently falls negative, maintaining a low average balance since opening. Deposits for the first 10 months do not exceed $2,600 with funds immediately being spent out of the account. Then several deposits over $6,000 are made prior to the fraudulent check of $25,680 just at the year-old mark for the account. This payer is carefully picked, having demonstrated solid traits:

- Medium size payer with activity seen across 3 financial institutions
- Average good check cleared over $33,000
- Sequence number of fraudulent check was within range of good items

Figure #6



Tenured Account Fraud (Accounts > 1 Year Old)

Tenured account fraud metrics:

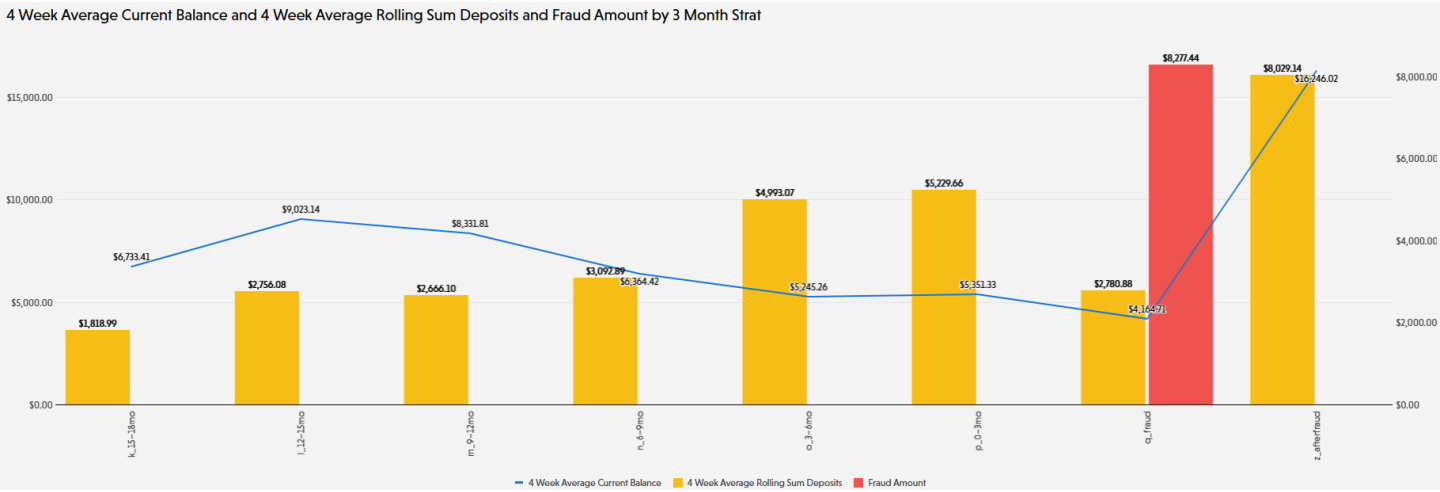
- Total percentage of check deposit dollars: 88.8%
- Total percentage of check deposit charge off dollars: 35.4%
- Fraud deposit rate: 0.07%
- Fraud detection rate: 87.2% (lowest fraud detection rate)

Finally, we have aged accounts, those that are greater than one year old. This segment makes up the lion's share of accounts and deposits as well as the percentage of good customers being scammed by fraudsters with fraudulent checks. It is here that we see the most complex fraud as it is fraught with good customers unknowingly aiding fraudsters, collaborating with fraudsters, scammed by the fraudster out of their own money, and ATO having their accounts taken over by the fraudster. As indicated by the lower fraud capture rate, it is most difficult for the financial institution to identify this type of fraud. This is particularly true when the customer is scammed or receives a bad check for payment as was identified as part of this analysis.

Tenured Account Fraud (> 1 Year Old)

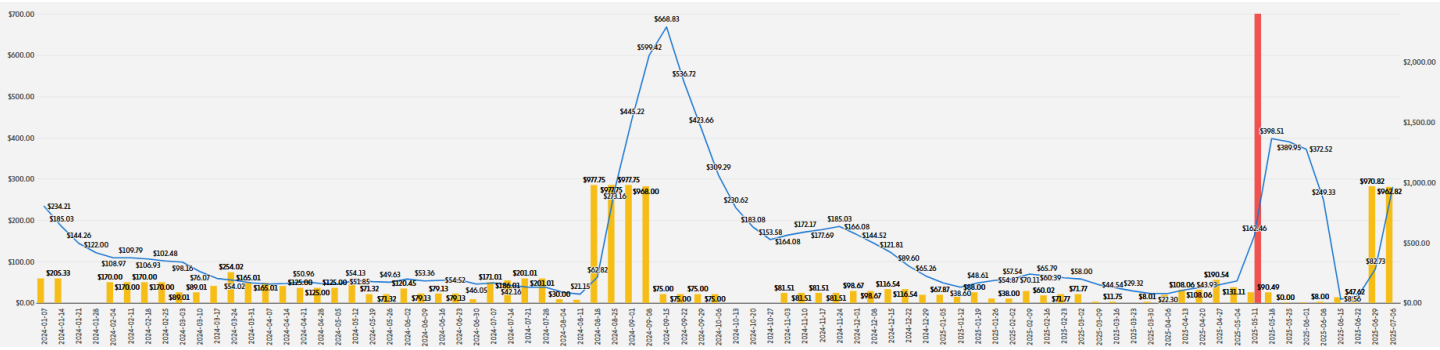
- *Significantly larger, average 4-week current balance above $5,000 prior to fraud event*
- *Consistent, monthly good deposits made > $2,500*
- *Average fraudulent check deposited is $8,277*
- *Deposits of $8,029 following the fraud event, signaling good customers replacing stolen balances following the scam*

Figure #7



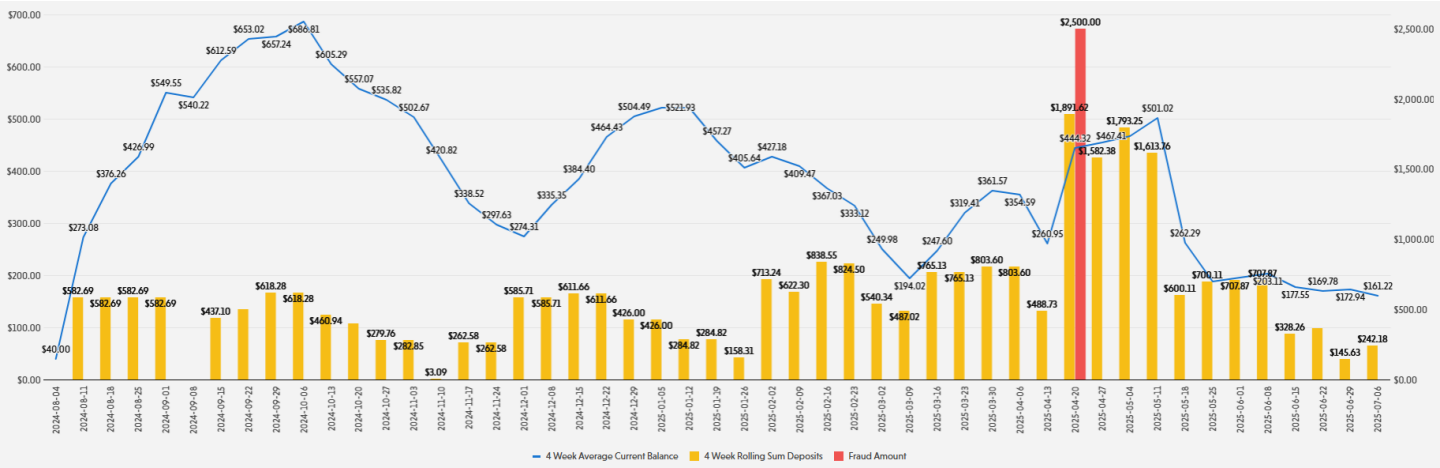
In the below example (figure #8), the account is just under 2 years old. Mostly smaller deposits with daily activity. Fraudulent check is deposited for $2,400, more than double any prior deposit from this account holder. The financial institution, having leveraged VALID alerts, rightly flagged this deposit and withheld the funds never suffered a loss. The client weeks later resumes normal deposit behavior and the bank retains the relationship while avoiding losses. This is a classic scenario where the customer was scammed by the fraudster, having no intention of defrauding the bank. Saving the customer from themselves, however, requires sophistication in the decisioning process.

Figure #8



During this same time period we saw additional fraud attempted on the same payer. While they are a small payer, they have a 7-year history of good payments with deposit activity identified across 4 different institutions. Fraud was attempted at two of the FI's multiple times, on both new and tenured accounts. The most tenured account holder to deposit a fraud check from this payer (see below in figure #9) is a 20-year-old account that fits a near identical profile of the 2-year-old account. Long, consistent activity with smaller deposits and low, fluctuating balances. Fraudulent check of $2,500 is deposited but good deposits immediately follow.

Figure #9



Conclusion

The findings from VALID and SentiLink's joint investigation make one fact clear: check deposit fraud is no longer a collection of isolated incidents — it is a highly organized, evolving ecosystem of attacks. Fraudsters exploit every phase of the account lifecycle, shifting tactics seamlessly from synthetic identities and first-party fraud in new accounts to sleeper strategies, social engineering, and account takeovers in tenured accounts. Key insights include:

- **Fraud Activity is Widespread and Organized**
  Every financial institution studied has seen significant fraud attempts with as much as **40% of deposited dollars in ATM by new accounts resulting in fraud returns**.

- **Fraud Evolves Over the Customer Lifecycle**
  Fraud tactics shift as accounts age, from **synthetic ID-driven new account fraud** to **collusion and account takeovers** in aged accounts.

- **Detection Effectiveness Declines Over Time**
  While financial institutions detect **97.4% of fraud** in new accounts, detection rates fall steadily to **87.2%** in accounts older than one year.

- **High-Risk Windows Exist Throughout Account Maturity**
  Fraudsters exploit **different vulnerabilities at different stages**, making a single, static fraud strategy insufficient.

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 consortium 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.

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

Additional Charts

Analysis of the check deposit fraud detection rate and fraud dollars attempted at several FI's representing over 50M unique accounts for full year 2024