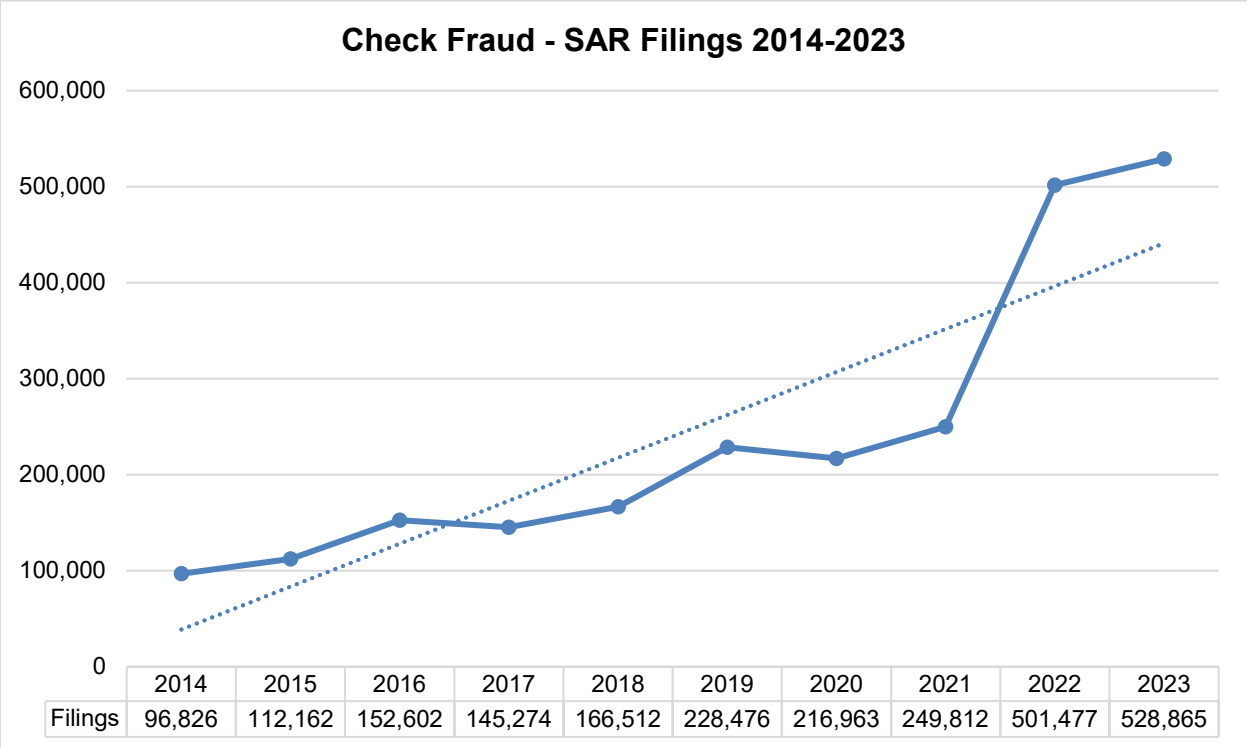
October 2024

RESOURCE PAPER: CHECK FRAUD AWARENESS & MITIGATION

Fraud losses for checks continues to be one of the most frequently reported claim types for financial institutions across the United States. This uptick in fraud is most surprising when you learn that check usage has been declining; the Federal Reserve reports that check collection has dropped 82% over the past 30 years[1].

The decreased volume of checks has also yielded a higher average check amount ($2,430) as most smaller transactions have migrated to ACH or debit card transactions[2]. Based on FinCEN filing data, check fraud has risen year over year since 2014 except for reporting years 2017 and 2020 where there was only a slight decrease, only to be followed by a dramatic increase. An important note is that these statistics only include check fraud that meets SAR filing requirements, the total picture of all check fraud is unknown. As of July 31, 2024, there have been 303,995 check fraud filings, trending towards 500,000+ filings for a third year in a row[3].



	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023
Filings	96,826	112,162	152,602	145,274	166,512	228,476	216,963	249,812	501,477	528,865

Check fraud dates to the 16th century and has gone through many iterations based on changes in the financial services marketplace, though some of the same general schemes are still utilized. Check kiting and washing have been around since the 1700's and, although we have made strides in the security measures for checks, these same techniques are being used by modern fraudsters[4]. With such a strong history, it appears that check fraud is not going to be slowing down anytime soon. This resource paper will outline some common check fraud schemes that we have seen and offer some best practice recommendations to mitigate fraud.

Where are the checks coming from?

Bad actors have obtained checks to perpetrate fraud in several ways, including but not limited to smash and grabs, home invasions and more recently directly from the United States mail system. Smash and grabs are a popular strategy for a gang called the "Felony Lane Gang", originally a gang from Florida that travels the country stealing identification cards and checkbooks from unattended cars often at gyms, daycares or parks. After checks and identification are stolen individuals wearing disguises approach victims' financial institutions and cash stolen checks from another victim's account. They are infamous for using the furthest lane in a drive thru, exploiting the fact that the camera quality and physical distance from tellers will make it harder to notice their wigs and other disguises[5].

More recently, the popular method of obtaining checks seems to be from the United States mail system. Since 2022, there has been an increase in the number of USPS letter carriers who have been robbed on the job. Bad actors are after the postal arrow keys which enables a bad actor to unlock postal boxes in the geographic region assigned. Once the key is obtained, the bad actors will use it to access incoming and outgoing mail, looking for envelopes that contain checks[6]. Bad actors have even bribed postal workers to assist them with stealing checks- USPS Office of the Inspector General indicated that individual have been prosecuted for aiding in the theft of Treasury Economic Impact Payments and another clerk who stole business checks[7]. The postal service is working to strengthen the security of the mail system with the addition of high security collection boxes and electronic locks, though these may take several years to fully implement[8].

Regardless of how the checks are originally stolen, often they will end up on the dark web for sale to other bad actors. The dark web enables bad actors to sell stolen checks to buyers across the world. Researchers from Georgia State University found that personal checks typically are sold for $175 and business checks for $250. In a two-month period, the same researchers located stolen checks with a face value of $22 million looking at only 60 online chat rooms out of several thousand[9].

What we are seeing

Much of the check fraud claims we see are tied to newly opened accounts [(New Account Fraud resource paper) PDF download]. Some accounts are first party fraud, where the applicant/future member is opening the account solely to perpetrate fraud. Other times the industry sees instances of identity theft and synthetic identity theft being used to open accounts using the personally identifiable information (PII) of another consumer. These accounts are higher risk as the financial institution may not have a complete understanding of the consumers' banking habits and may grant products and services based solely on the fact that they qualified for an account. Because the financial institution does not have an established relationship and a complete understanding of what is "normal" for the new account holder, it would be appropriate for the financial institution to consider incorporating underwriting techniques and tiers for higher risk services such as ATM deposit capability and Remote Deposit Capture services. These channels are popular for fraud because there is an element of anonymity for the individual making the deposit, believing that the item will have a greater chance of slipping through the cracks without review.

Check fraud is not limited to only new accounts, the industry sees quite a bit of fraud on established accounts. Fraud on established accounts is often tied to checks being stolen and washed, being negotiated by someone other than the original payee and for different amounts. We also see established accounts being taken over by bad actors who have an account holder's identification card or other official documents to make deposits and subsequent cash withdrawals, often using the drive-through lanes.

Beginning in the fall of 2023, there was an uptick in check fraud with treasury checks. These large checks were sent to businesses for the Employee Retention Credit (ERC), a program tied to the Coronavirus Aid, Relief, and Economic Security (CARES) Act. These paper checks were sent by mail to businesses who met certain requirements, unfortunately they were intercepted enroute to the intended payees. Because bad actors can easily identify treasury checks in the mail the scheme has continued with the theft of any treasury checks including tax refunds. Fraud tied to treasury checks has typically fallen into three buckets:

1. Use of legitimate but stolen treasury check deposited into account opened in the name of the original payee on the treasury check (Using Identity theft).
2. Altering (Washing) the payee of the check to a new payee.
3. Negotiating counterfeited treasury checks utilizing the treasury check stock designs.

In most cases of treasury check fraud, the deposit is made into a new account, and the date of the check will pre-date the account opening date. Our Risk Alert, Fraudulent United States Treasury Check Deposits (PDF download), contains additional

information relating to this scheme. It is especially important to spot fraudulent treasury checks because the Treasury has up to 18 months for the reclamation action to take place[10].

Risk Mitigation Best Practices

According to the 2024 AFP Payments Fraud and Control Survey Report, 65 percent of organizations faced fraudulent check activity on their accounts in 2023[11]. It is only a matter of time before an organization (including a financial institution) becomes a victim of check fraud. One of the best prevention tools to protect a commercial account against fraudulent checks being negotiated is by using a Positive Pay system or ideally a Payee Positive Pay system. When checks are presented for clearing and settlement, these systems will allow only items that match information that has been previously provided as legitimate. It will ensure that the check number, account number and dollar amount match what is on file, Payee Positive Pay goes a step further to ensure that the payee's name matches to spot washed checks. Positive pay is a function that should be utilized on all financial institutions, corporate checks, official checks and cashiers' checks. The service can also be offered to business accountholders because their checks are often targeted by bad actors.

With bad actors using technology to commit their fraud, it is important that a financial institution also leverage technologies to counter the fraud. There are several check fraud specific software solutions that use databases of known fraud elements to alert and advise you in real time to potential check fraud. These tools should be deployed for all channels of check acceptance (in-branch, ATM, and RDC). It is also critical that the financial institution have a robust fraud monitoring system that looks at not only check activity to spot potential issues with an account.

Of course, keeping your entire staff (especially front-line tellers), fully abreast of current fraud trends will be one of the best lines of defense to protect against check fraud losses. The employees of your financial institution, including front-line staff, play a pivotal role in detecting and preventing check fraud. Front-line staff typically have the most interaction with accountholders and should be able to recognize what is "normal" behavior for a particular accountholder. Any check or account activity that is out of the norm should be escalated to your fraud or risk team for further investigation.

The Risk Management Team with Allied Solutions releases risk alerts and resources on emerging fraud and risk categories. We encourage everyone at your financial institution to subscribe and receive fraud newsletters and just-in-time risk alerts straight to your inbox.

[1] https://www.bostonfed.org/news-and-events/news/2023/08/check-fraud-rampant-mike-timoney-column-fraud-awareness-key-to-slowing-surge.aspx
[2] https://www.federalreserve.gov/paymentsystems/fr-payments-study.htm
[3] https://www.fincen.gov/reports/sar-stats
[4] https://www.acfe.com/fraud-resources/fraud-examiner-archives/fraud-examiner-article?s=check-fraud-evolution
[5] https://www.ice.gov/news/releases/leader-floridas-million-dollar-felony-lane-gang-sentenced-more-15-years-prison
[6] https://about.usps.com/newsroom/national-releases/2023/0512-usps-postal-inspection-service-roll-out-expanded-measures-to-crack-down-on-mail-theft.htm
[7] https://www.uspsoig.gov/investigative-work/case-highlights/opportunity-makes-thief
[8] https://about.usps.com/who/government-relations/assets/project-safe-delivery-postal-101.pdf
[9] https://www.web.abrigo.com/check-fraud-dark-web
[10] https://tfx.treasury.gov/tfm/volume1/part4/chapter-7000-cancellations-deposits-reclamations-and-claims-checks-drawn-us
[11] https://www.afponline.org/training-resources/resources/survey-research-economic-data/Details/payments-fraud