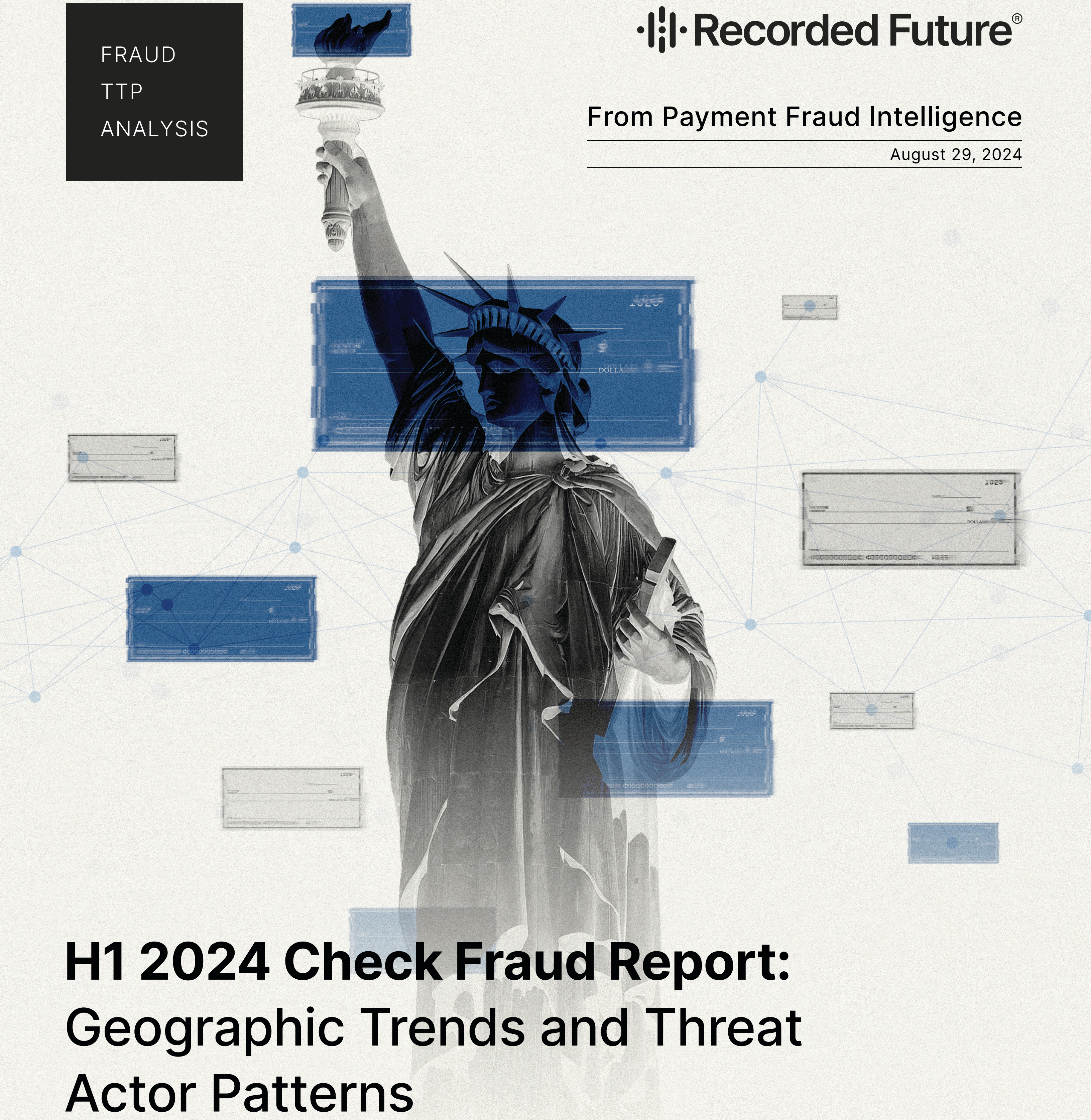
FRAUD
TTP
ANALYSIS

Recorded Future®

From Payment Fraud Intelligence

August 29, 2024



H1 2024 Check Fraud Report: Geographic Trends and Threat Actor Patterns

Mail theft-related check fraud has exploded in recent years. Recorded Future's Payment Fraud intelligence Team analyzed one million stolen bank check images posted for sale on 700 Telegram sources.

Rampant reposting defines this check fraud ecosystem. For every new stolen check posted for sale, we observed an average of six reposts on other channels.

Geographical analysis indicated that in New York City, numerous threat groups likely conduct mail theft. In smaller cities like Baton Rouge, only one or two threat groups are likely responsible.

Executive Summary

Check fraud — a threat vector in which fraudsters steal, counterfeit, and forge checks — has exploded in the US over the past 3 years. The US Department of the Treasury has reported a 90% increase in check fraud-related suspicious activity reports (SARs) from 2021 to 2023, an increase that maps onto an estimated $21 billion in consumer and business losses in 2023. The sharp rise of check fraud has been supported by the growth of a local, US-based cybercriminal ecosystem that primarily uses messaging apps like Telegram to connect buyers and sellers.

To determine the areas most impacted by the increase in check fraud and the sources driving the increase, Recorded Future's Payment Fraud Intelligence team analyzed nearly one million stolen bank check images that were posted on over 700 Telegram sources in H1 2024. Analysis in this check fraud report revealed three major check fraud statistics and trends:

- The check fraud ecosystem on Telegram is defined by rampant reposting
- Threat actors post stolen check images soon after stealing the checks
- Stolen checks impact all 50 US states, with the highest density along the Eastern Seaboard

For financial institutions, the sharp increase in check fraud translates to mounting direct fraud losses and rising indirect operational expenses borne by anti-fraud and customer service assets. Tools like Recorded Future Bank Check Data provide financial institutions with structured stolen bank check data, equipping them to protect at-risk accounts, proactively block fraudulent deposits and withdrawals, and partner with law enforcement to prosecute individuals involved in check and deposit fraud.

Key Findings

- Stolen check images regularly appear on multiple Telegram channels: for every original and net-new check image, we observed an average of six reposts of the check on other Telegram channels.
- 50% of stolen check images are posted within eight days of when the check was signed, and 75% of stolen checks are posted to Telegram within two weeks.
- Major metropolitan areas of the US saw the highest concentrations of stolen checks. A case study of New York City revealed that the top source of new, non-reposted checks varied across ZIP Codes, indicating that numerous threat groups are likely operating across the city.
- Check theft occurrences in suburban and rural areas across the US indicate check fraud is not exclusively a threat in major metropolitan areas. A case study of Baton Rouge and neighboring St. Landry Parish in Louisiana revealed a spike in the theft of US Treasury checks coinciding with the tax season.

Threat Analysis

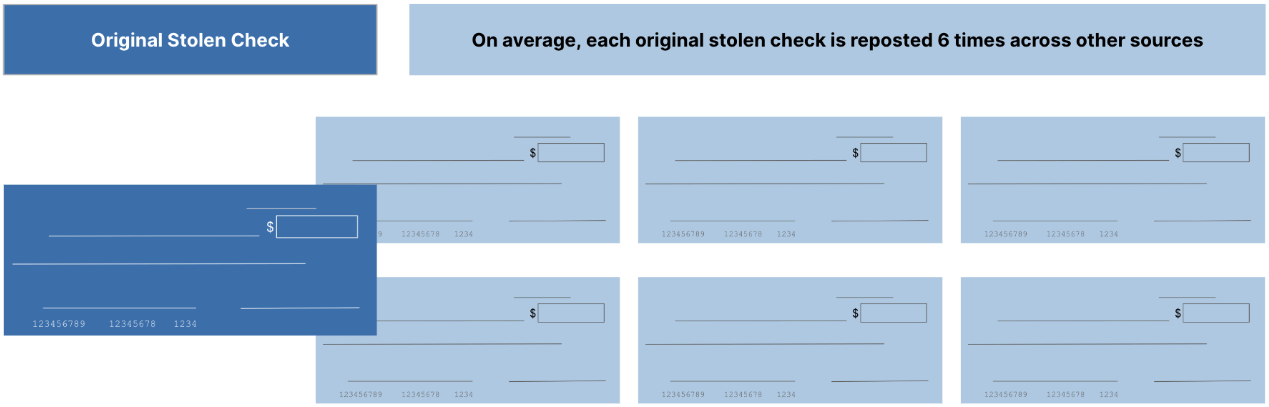
At a high level, check fraud entails the theft, "washing", and cash-out of fraudulent checks via deposit fraud. In a dynamic paralleling the more established card fraud ecosystem, threat actors have increasingly diversified into "suppliers" (who steal the checks) and "buyers" (who deposit and cash out stolen checks themselves or coordinate the activity via criminal associates and unwitting accomplices). To facilitate exchange, Telegram channels have emerged as the primary check fraud marketplaces where suppliers post images of stolen checks to attract buyers.

To surface geographic check fraud hotspots and the sources fueling them, Recorded Future's Payment Fraud Intelligence team compiled check fraud statistics by analyzing nearly one million stolen bank check images that were posted on over 700 Telegram sources in H1 2024.

Check Fraud Ecosystem on Telegram Defined by Rampant Reposting

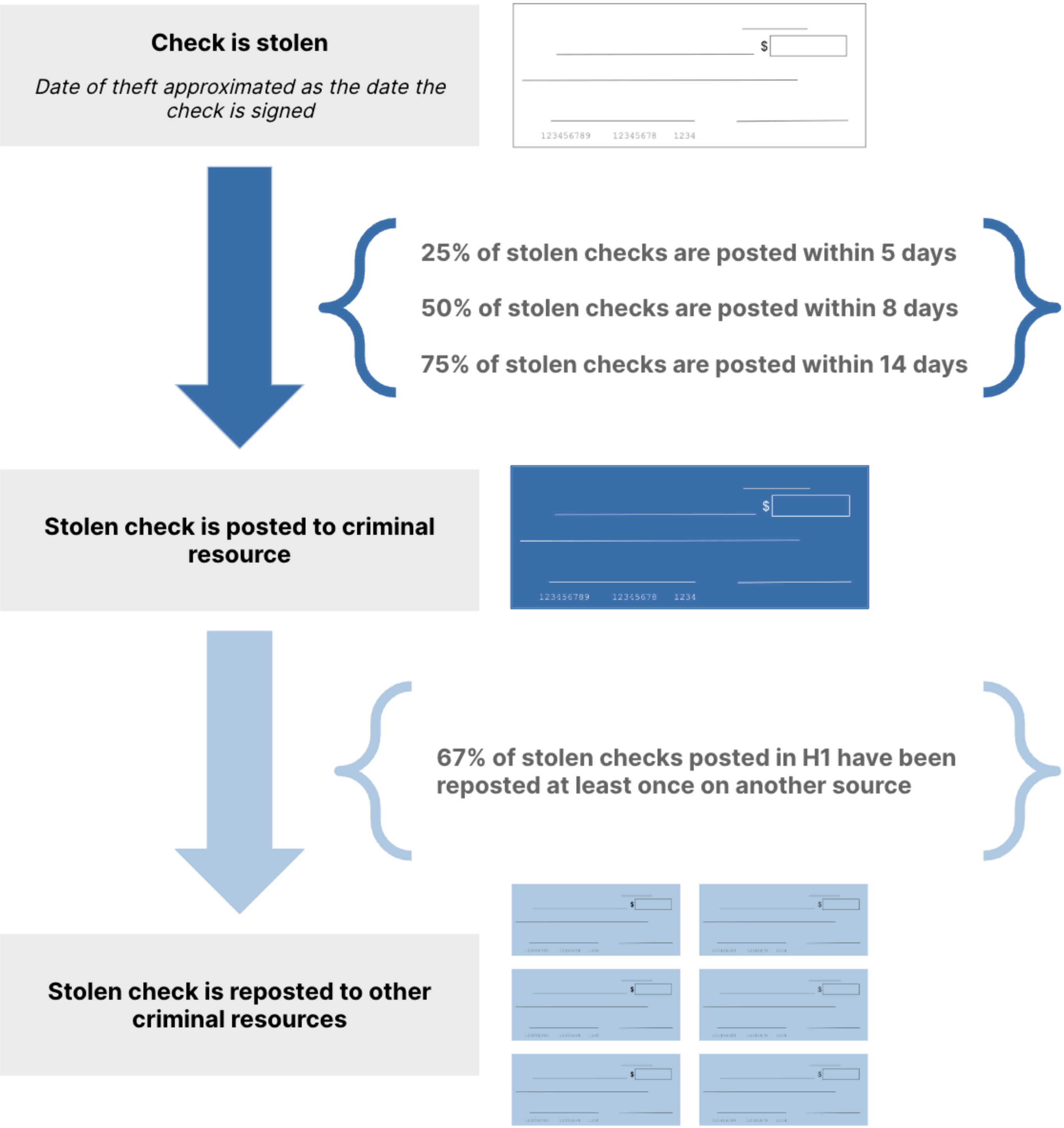
A powerful finding of this check fraud report, analysis of checks posted to Telegram in H1 2024 revealed that 85% are likely "reposts", indicating a threat actor either advertised the check on multiple sources or reposted another threat actor's stolen check image for their own purposes.

The common practice of reposting stolen check images creates a cacophony of signals for defenders triaging *unstructured* check images. The cacophony complicates efforts to convert counts of raw stolen check images into a leading indicator for check fraud and consumes valuable resources on deduplication efforts. *Structured* stolen check data provides a through-line to the most important segment: the original stolen check images.


Original Stolen Check
On average, each original stolen check is reposted 6 times across other sources
$
123456789 12345678 1234

Half of Stolen and Fraudulent Checks Appear on Telegram within Eight Days

Stolen checks frequently appear on Telegram within days of when they were likely stolen. Once a stolen check appears on one source, reposted versions of it typically appear on other sources in the following days.



Check is stolen

Date of theft approximated as the date the check is signed

25% of stolen checks are posted within 5 days

50% of stolen checks are posted within 8 days

75% of stolen checks are posted within 14 days

Stolen check is posted to criminal resource

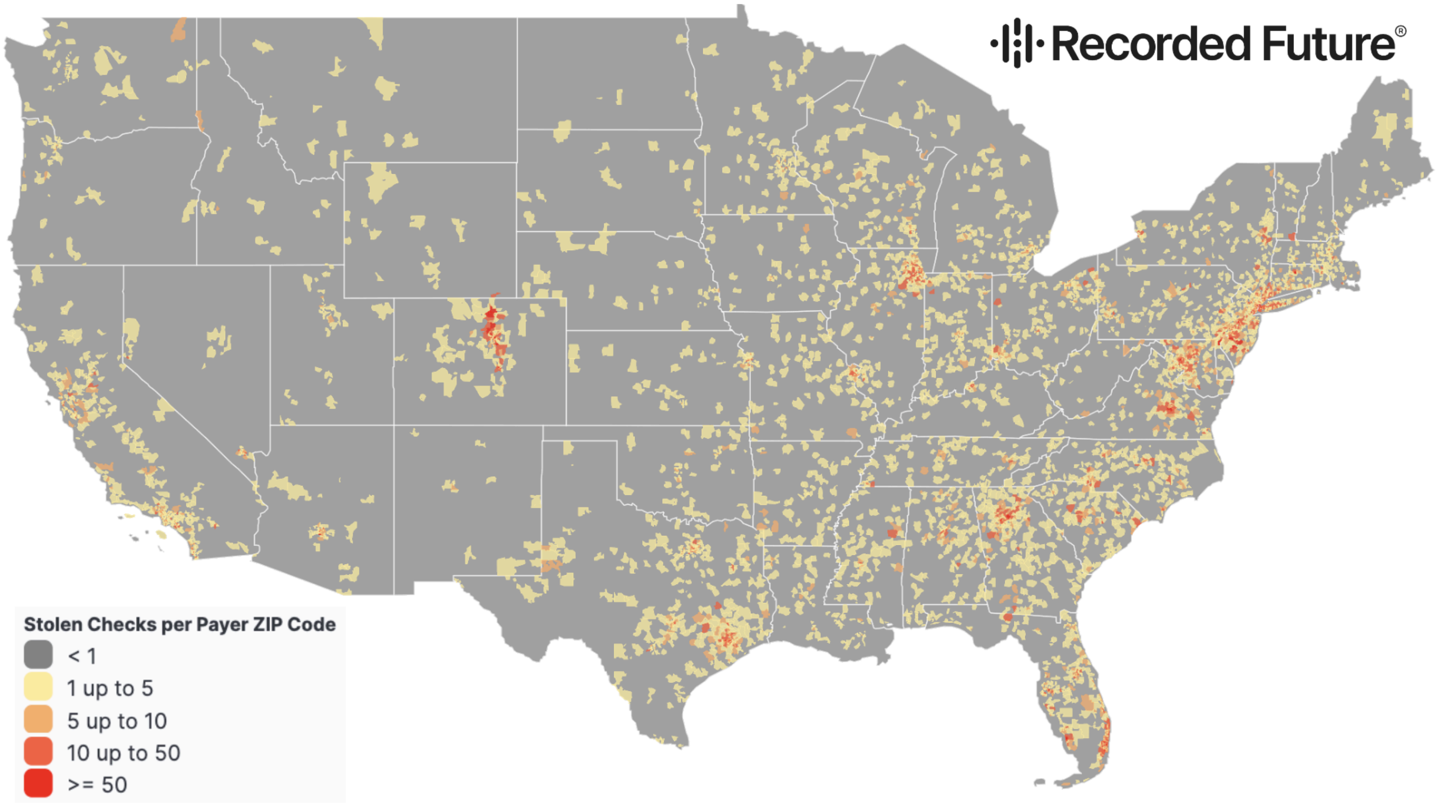
67% of stolen checks posted in H1 have been reposted at least once on another source

Stolen check is reposted to other criminal resources

Stolen Checks Impact Nation, H1 Density Highest Along Eastern Seaboard

A check can be stolen at any point between when an individual drops it into a mailbox and when the recipient has it in their hand. Focusing on the geodata of stolen checks' payer (the address information of the person sending the check) helps surface concentrations in specific locations, and layering in the source of the stolen checks for those locations generates leads for threat actor attribution.

At a surface level, states and cities with large populations are typically responsible for the highest share of stolen checks. Nevertheless, as shown below, we've observed numerous hot spots outside of the largest US cities, indicating that check fraud is not exclusively a threat in major metropolitan areas.



Although not visualized above, the geodata of stolen checks' payees (the address information of the person receiving the check) is also concentrated around major urban areas, generally correlating with the geodata of payers. At face value, this correlation complicates efforts to forecast whether payee-based concentrations likely represent check theft events occurring once the checks arrive within the payee location (e.g., a recipient post office or from mailboxes and mail rooms).

However, as explored in this check fraud report's two case studies below, analysis of ZIP Codes with payee concentrations disproportionately higher than payer concentrations reveals areas in which threat actors are likely stealing checks on the delivery side. In the case study looking at Baton Rouge and St. Landry Parish, Louisiana, this dynamic is clearly seen in relation to the theft of US Treasury checks.

Case Study #1: Check Fraud Statistics for New York City, New York

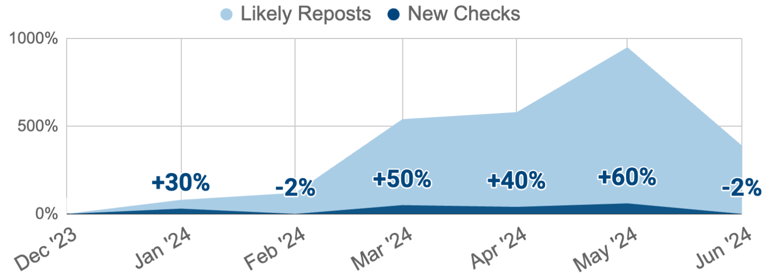
Top Target of Check Fraud, Numerous Threat Groups

The raw volume of stolen checks sent from and to New York City increased over H1. The underlying segment of new, non-reposted checks rose in the spring, largely on the back of stolen US Treasury checks.

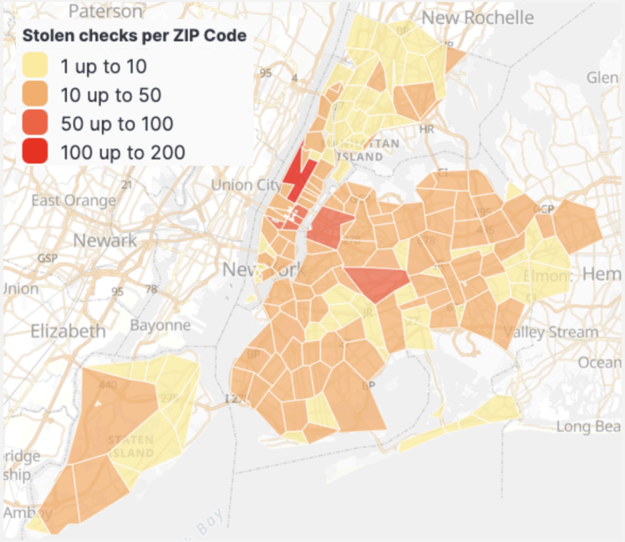
The top sources of new, non-reposted checks varied across ZIP Codes. They were rarely responsible for a majority of stolen checks in the ZIP Code, indicating numerous threat groups are operating across the city.

New York City, NY

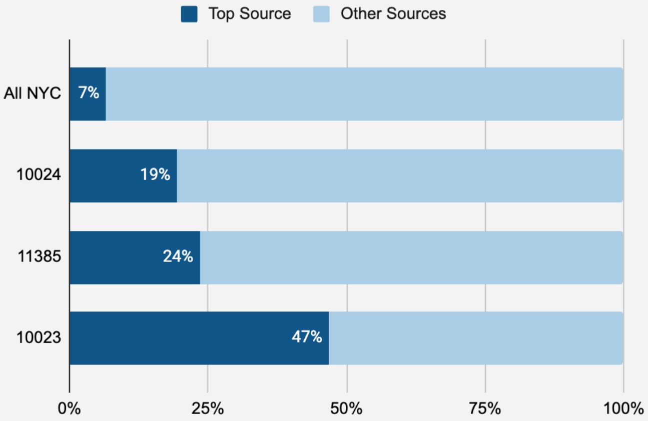
H1 2024 Monthly Stolen Check Volumes vs. December 2023



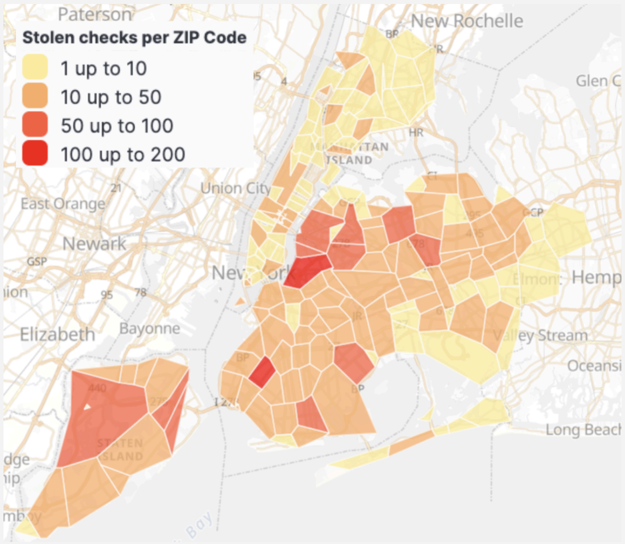
NYC: Payer Data



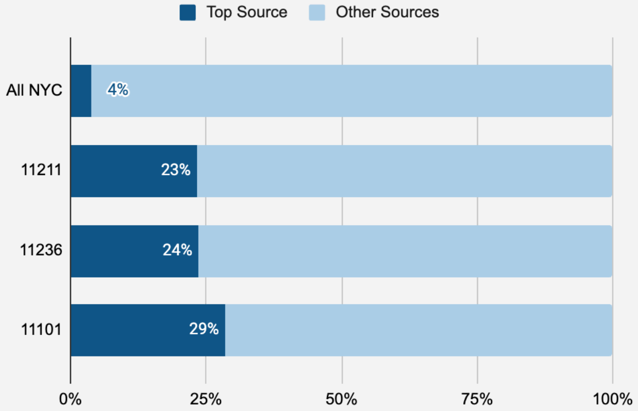
Top Source's Share of Unique Checks



NYC: Payee Data



Top Source's Share of Unique Checks

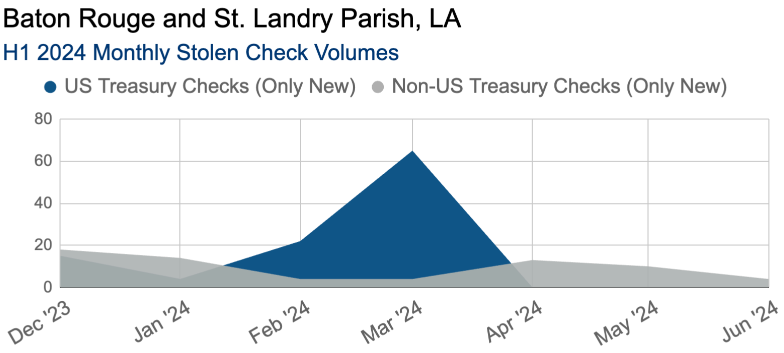


Case Study #2: Check Fraud Statistics for Greater Baton Rouge, Louisiana

Spike in US Treasury Check Theft Concentrated Around a Few Sources

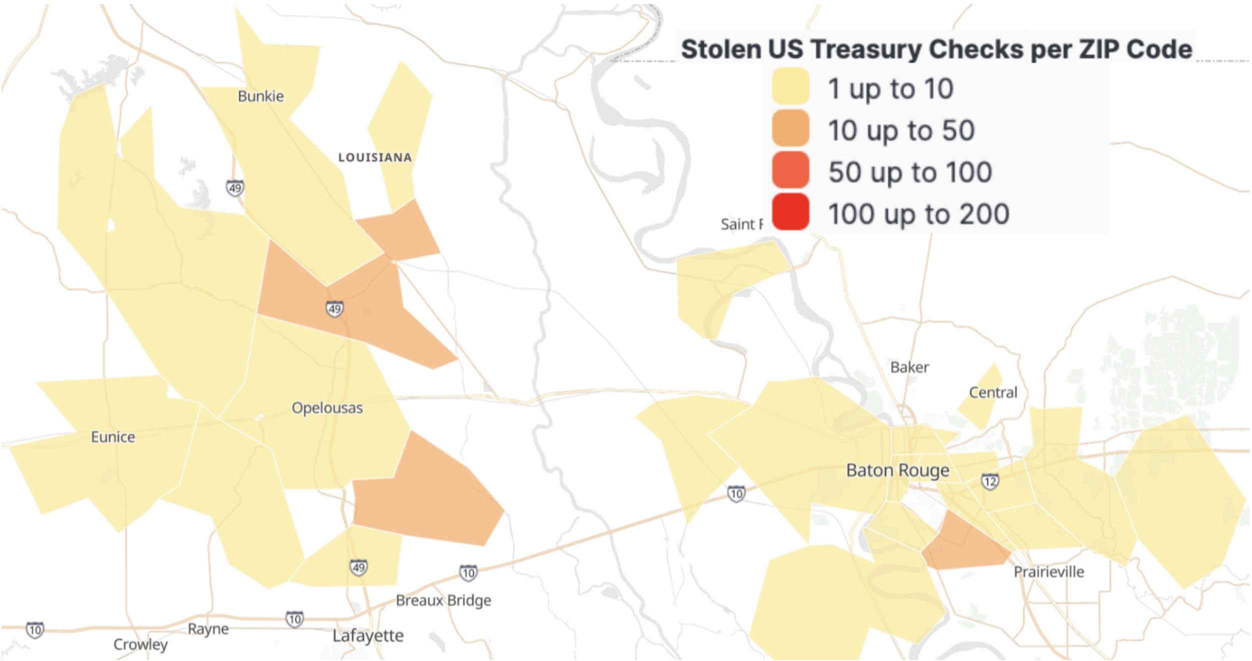
When examining only new checks and filtering out reposted checks, Baton Rouge and St. Landry Parish in Louisiana saw a spike in stolen checks in February and March 2024. The stolen checks were overwhelmingly US Treasury checks, coinciding with the tax season and the disbursal of tax refunds.

Unlike New York City, the stolen checks from this area were more heavily concentrated around several sources, indicating one or two threat groups were likely responsible for the majority of theft.

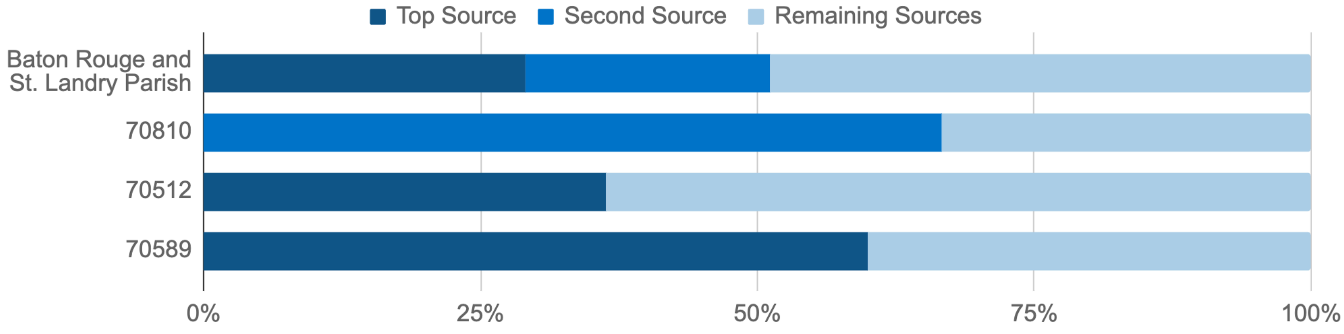

Baton Rouge and St. Landry Parish, LA

H1 2024 Monthly Stolen Check Volumes

Stolen US Treasury Check and Source Density by Payee Data



Top Sources' Share of US Treasury Checks



Mitigations

Financial institutions should mitigate check fraud by educating customers, developing and applying stolen check fraud intelligence to prevent deposit fraud, and collaborating with law enforcement.

- Inform customers about the risk of check fraud and provide customers with easy-to-use guides that detail how to use alternative payment methods. Checks are often sent through the mail to pay utilities, landlords, service providers, and corporate suppliers. However, the growth of online bill pay options and money transfer services — including traditional wire transfers and newer options like Zelle — provide individuals and organizations with a safer alternative to mailing checks.
- Ingest Recorded Future Bank Check Data to (1) match outbound stolen checks to customer accounts and (2) screen inbound check deposits to combat deposit fraud. Matching outbound stolen checks to customer accounts prevents customers from suffering fraud losses, whereas screening inbound check deposits prevents your financial institution from accepting — and later reimbursing — stolen funds.
- Compile check fraud statistics and submit suspicious activity reports (SARs) to enable law enforcement to investigate threat actors that traffic in fraudulent checks and perpetuate check fraud.

Outlook

Check fraud statistics — measured both in reported fraud instances and aggregate fraud losses — have sharply increased in the US despite a decrease in overall check usage. According to the US Federal Reserve, the volume of commercial checks collected through the Federal Reserve nearly halved from 2013 to 2023 as the average value of each of those checks more than doubled. Similarly, the 2022 Federal Reserve Payments Study estimated that from 2012 to 2021, the volume of consumer checks declined as the aggregate value of check transactions flatlined.[1] Ultimately, check fraud's documented rise in the face of declining check usage makes it unrealistic to expect that declining check usage alone will solve the problem of check deposit fraud in the short term.

Looking forward, the only factor that is likely to moderate the threat posed by check fraud is financial institutions' ability to adopt improved check verification and anti-fraud processes. Employed effectively at an industry-wide level, these barriers would likely disincentivize cybercriminals from engaging in check fraud, which has otherwise proven profitable enough to prop up a cottage industry of messenger-based, fraud-focused criminal communities specializing in the sale of fraudulent checks. Beyond these bank-centric processes, we have no evidence to suggest that the key factors enabling check fraud — including insider threats, unmonitored mail drop boxes, commercially available solvents for "washing" checks, and willing money mules to deposit stolen checks — will disappear any time soon.

[1] In 2018, The US Federal Reserve estimated that it processes one-third of all checks in the US.

Recorded Future reporting contains expressions of likelihood or probability consistent with US Intelligence Community Directive (ICD) 203: Analytic Standards (published January 2, 2015). Recorded Future reporting also uses confidence level standards employed by the US Intelligence Community to assess the quality and quantity of the source information supporting our analytic judgments.

About Insikt Group®

Recorded Future's Insikt Group, the company's threat research division, comprises analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence that reduces risk for clients, enables tangible outcomes, and prevents business disruption.

About Recorded Future®

Recorded Future is the world's largest threat intelligence company. Recorded Future's Intelligence Cloud provides end-to-end intelligence across adversaries, infrastructure, and targets. Indexing the internet across the open web, dark web, and technical sources, Recorded Future provides real-time visibility into an expanding attack surface and threat landscape, empowering clients to act with speed and confidence to reduce risk and securely drive business forward. Headquartered in Boston with offices and employees around the world, Recorded Future works with over 1,800 businesses and government organizations across more than 75 countries to provide real-time, unbiased, and actionable intelligence.

Learn more at recordedfuture.com