

FINANCIAL CRIMES ENFORCEMENT NETWORK



Financial Trend Analysis

**Mail Theft-Related Check Fraud:
Threat Pattern & Trend Information,
February to August 2023**

September 2024



Mail Theft-Related Check Fraud: Threat Pattern & Trend Information, February to August 2023

This Financial Trend Analysis focuses on patterns and trends identified in Bank Secrecy Act (BSA) data linked to mail theft-related check fraud. The Financial Crimes Enforcement Network (FinCEN) is issuing this report pursuant to section 6206 of the Anti-Money Laundering Act of 2020, which requires periodic publication of BSA-derived threat pattern and trend information.¹ FinCEN issued government-wide priorities for anti-money laundering and countering the financing of terrorism (AML/CFT) on 30 June 2021, which included fraud as a government-wide priority. The United States (U.S.) Department of the Treasury established mail theft-related check fraud as a concern, and FinCEN issued the Alert on Nationwide Surge in Mail Theft-Related Check Fraud Schemes Targeting the U.S. Mail, FIN-2023-Alert 003, on 27 February 2023 (February 2023 Mail Theft-Related Check Fraud Alert).² This Financial Trend Analysis is relevant to the public and a wide range of consumers, businesses, and industries and it highlights the value of BSA information filed by regulated financial institutions, including responses to the February 2023 Mail Theft-Related Check Fraud Alert.

Executive Summary: This Financial Trend Analysis analyzes threat pattern and trend information on mail theft-related check fraud incidents, based on BSA data filed with FinCEN between 27 February and 31 August 2023 (the review period).³ During the review period, FinCEN received 15,417 BSA reports related to mail theft-related check fraud associated with more than \$688 million in transactions, which may include both actual and attempted transactions. Mail theft-related check fraud losses can affect personal savings, checking accounts, business accounts, brokerage accounts and retirement savings, as well as negatively impact financial institutions that typically cover check fraud losses.

Scope and Methodology: FinCEN examined BSA reports that used the February 2023 Mail Theft-Related Check Fraud Alert key term filed during the review period to determine trends. The February 2023 Mail Theft-Related Check Fraud Alert requested financial institutions include the term “FIN-2023-MAILTHEFT” in BSA reporting. The full data set consisted of 15,417 BSA reports filed during this review period, reporting roughly \$688 million in mail theft-related check fraud incidents, which may include both completed and attempted

1. William M. (Mac) Thornberry Nat'l Def. Authorization Act for FY 21, Pub. L. No. 116-283, division F, §§ 6001-6511 (2021).
2. See Department of the Treasury, “National Money Laundering Risk Assessment” February 2024, <https://home.treasury.gov/system/files/136/2024-National-Money-Laundering-Risk-Assessment.pdf>.
3. See “FinCEN Alert on Nationwide Surge in Mail Theft-Related Check Fraud Schemes Targeting the U.S. Mail,” FinCEN Alert #FIN-2023-Alert003, 27 February 2023, FinCEN Alert, [FIN-2023-Alert003, February 27, 2023](https://www.fincen.gov/alerts/fin-2023-alert003).

FINANCIAL TREND ANALYSIS

transactions.^{4 5} These reports may refer to incidents that occurred prior to the review period. FinCEN used a combination of automated and manual review of mail theft-related check fraud BSA reports to identify mail theft-related check fraud activity.

Overview of Key Findings: FinCEN identified three primary outcomes from perpetrators after stealing checks from the U.S. Mail: (1) altering and depositing the checks, (2) using the stolen checks to create counterfeit checks, and (3) fraudulently signing and depositing the checks. The methodologies that criminals use to perpetrate these outcomes can range from unsophisticated to highly organized and complex, often involving the use of advanced counterfeit check technology and chemicals that can remove ink from stolen checks.

- ✓ *Banks Filed 88 percent of All Mail Theft-Related Check Fraud Reports:* The largest banks (by asset totals) in the United States submitted 44 percent of the bank filings in the review period. Small-to-medium size banks filed a majority of BSA reports on mail theft-related check fraud.
- ✓ *Checks are Most Frequently Altered and then Deposited After They are Stolen from the Mail:* Criminals most frequently alter and then negotiate stolen checks, according to BSA reporting.⁶ Their second most frequent use of stolen checks was creating counterfeit checks—where a stolen check is used as a template to produce counterfeits. And the third most common outcome was perpetrators fraudulently signing and depositing checks.⁷ Altered checks accounted for approximately 44 percent of the BSA reports, counterfeit accounted for 26 percent, and fraudulently signed checks were 20 percent, according to manual review of BSA reports.
- Methodologies Range in Sophistication:* The level of sophistication of the check fraud depends on the perpetrator's technological capabilities. Effective alterations and counterfeit checks require some knowledge of the technology and chemicals used to wash checks.⁸
- ✓ *Reliance on Avoiding Human Contact:* Many perpetrators utilized methods that avoid human contact, including check deposits via remote deposit capture (RDC) or at automated teller machines (ATMs) and opening accounts online rather than in person.

4. Amounts associated with these BSA reports may include attempted transactions and payments that were unpaid. This figure also includes BSA reports that describe continuing suspicious activity or amend earlier reporting, or reports that cover expanded networks involved in potential illicit activity. These suspicious activity amounts may also include duplicates, counting of both inbound and outbound transactions, transfers between accounts, typos, and errors as submitted by filers. Additionally, to reduce outliers, FinCEN excluded amounts over \$1 billion, which caused the loss of two BSA reports.
5. For the purposes of this report, FinCEN omitted filings pertaining to August 2023 incidents filed after the review period.
6. Check negotiation refers to a transfer of ownership of a check or the process of changing a check into money. It can also include endorsing a check and depositing it, cashing it, or signing it over to another party for further negotiation.
7. These figures represent the number of times a methodology was identified for individual check deposits reported in BSA data. BSA reports indicated multiple check deposits in one report that may detail different methodologies. As such, the numbers for each methodology will be higher than the total number of BSA reports reviewed.
8. Check washing is when criminals treat a stolen check with chemicals or compounds that remove the ink from a check and then replace the erased information.

FINANCIAL TREND ANALYSIS

- *Mail Theft-Related Check Fraud is a Nationwide Problem:* The BSA reporting included subjects or branch activity in every U.S. state as well as Washington, D.C., and Puerto Rico.

What is Mail Theft-Related Check Fraud?

Mail theft-related check fraud is the fraudulent negotiation of checks stolen from the U.S. Mail.⁹ Criminals may steal different types of checks and attempt to use them for their own benefit. Once stolen, there are several ways they use the checks, including altering payees and/or amounts, using the stolen check to create counterfeit checks, fraudulently signing the check, and selling the check or its identifying information on dark web marketplaces or encrypted social media platforms, according to BSA reporting. Generally, mail theft-related check fraud is the combination of two crimes: mail theft and check fraud.

The United States Postal Inspection Service (USPIS) received 299,020 mail theft complaints between March 2020 and February 2021, a 161 percent increase compared with the previous 12 months.¹⁰ Additionally, the United States Postal Service (USPS) reported 38,500 high volume mail theft incidents from mail receptacles (including blue USPS collection boxes) from October 2021-October 2022 and over 25,000 such incidents in the first half of Fiscal Year 2023.¹¹ While mail theft often consists of mail being stolen from USPS mailboxes or personal mailboxes, USPIS reported 412 mail carriers were robbed on duty between October 2021-October 2022 and 305 were robbed in the first half of Fiscal Year 2023.¹² Incidents of mail theft spiked after the onset of the COVID-19 pandemic, as many individuals and businesses received financial assistance via the U.S. Mail.¹³

Check fraud refers to any use of paper or digital checks to fraudulently obtain funds. As noted above, this fraud can take many forms, including alterations, counterfeiting, and perpetrators signing checks not belonging to them, among others. FinCEN received over 680,000 BSA filings related to check fraud in 2022, which is nearly double the filings received related to check fraud in the previous year.¹⁴ Those filings cover check fraud as a whole and are not indicative of mail theft-related check fraud, specifically.

9. See FinCEN *supra* note 3.

10. See "U.S. Postal Inspection Service Pandemic Response to Mail Fraud and Mail Theft," U.S. Postal Service Office of the Inspector General Report #20-305-R21, 20 May 2021, <https://www.uspsoig.gov/sites/default/files/reports/2023-01/20-305-R21.pdf>.

11. See USPS, "Postal Inspection Service Roll Out Expanded Crime Prevention Measures to Crack Down on Mail Theft, Enhance Employee Safety, and Strengthen Consumer Protections," 12 May 2023, <https://about.usps.com/newsroom/national-releases/2023/0512-usps-postal-inspection-service-roll-out-expanded-measures-to-crack-down-on-mail-theft.htm>.

12. See *id.*

13. See USPS *supra* note 10.

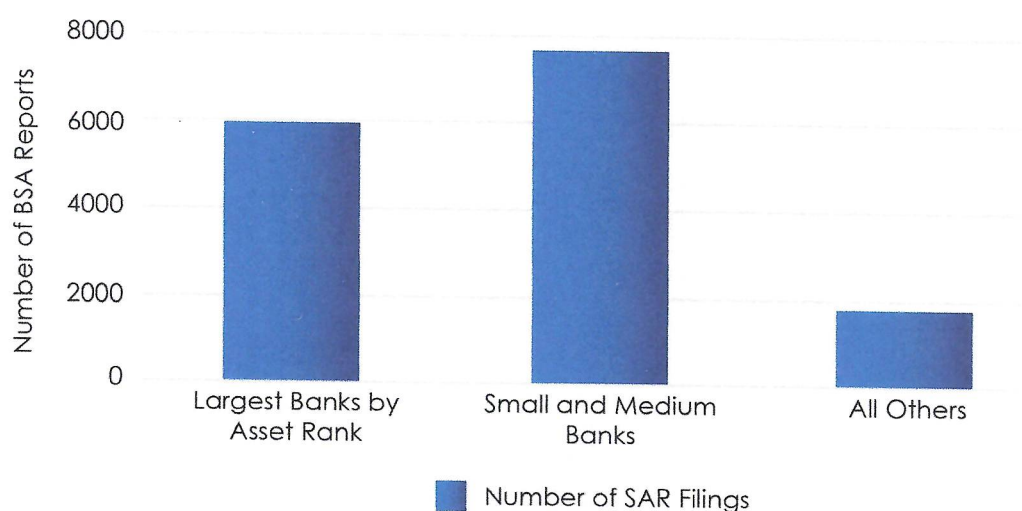
14. See FinCEN *supra* note 3.

Banks Filed Vast Majority of Mail Theft-Related Check Fraud BSA Reports

Financial institutions filed 15,417 BSA reports with the February 2023 Mail Theft-Related Check Fraud Alert key term during the review period. This period covers the first six months after FinCEN issued its alert to use the key term in BSA filings on 27 February 2023. A total of 841 financial institutions—consisting primarily of banks, credit unions, and securities/futures firms—filed BSA reports indicating the mail theft-related check fraud alert term. The number of filings each month were relatively consistent during the review period, ranging from a low of 2,307 received in July 2023, to a high of 2,918 received in August 2023.

Banks filed 13,618 of the total mail theft-related check fraud BSA reports, accounting for 88 percent of the filings during the review period. The largest U.S. banks by asset size, according to rankings by the Federal Reserve, filed 44 percent of the BSA reports from banks.¹⁵ In total, 635 unique banks filed BSA reports indicating mail theft-related check fraud, which included 31 banks that filed more than 100 BSA reports during the review period. Financial institutions that filed BSA reports in this dataset included instances when clients were victimized and when clients deposited or attempted to deposit stolen or counterfeit checks.

BSA Report Filings by Filer Type



While credit unions and securities/futures firms also issue and negotiate checks, these financial institutions combined only filed 1,767 BSA reports—or 11.5 percent of the total—during the review period. Securities/futures firms filed 885 BSA reports, and credit unions filed 882 BSA reports. In total, 32 different securities/futures firms and 165 different credit unions filed mail theft-related check fraud BSA reports.

15. See “Insured U.S-Chartered Commercial Banks that have Consolidated Assets of \$300 Million or More, Ranked by Consolidated Assets as of March 31, 2023,” Federal Reserve Statistical Release, United States Federal Reserve Board, <https://www.federalreserve.gov/releases/lbr/current/>.

Money services businesses (MSBs) filed three mail theft-related check fraud BSA reports. While this may represent a relatively low number of BSA reports, check casher MSBs are not required to file Suspicious Activity Reports, although they may do so voluntarily. Check cashers, however, are required to register with FinCEN as an MSB, maintain an anti-money laundering program, and meet other recordkeeping and reporting obligations under the BSA.¹⁶

The average activity amount reported per BSA report for mail theft-related check fraud was \$44,774, while the median amount was \$14,215. This included 41 BSA reports that had no amount reported, 41 others that reported \$0, and one that reported \$1.¹⁷ Additionally, numerous BSA filings reported the entire amount of a check that was attempted to be negotiated, even though the transaction never occurred.

✓ **Stolen Checks are Most Frequently Altered Before Negotiation**

Stolen checks are most frequently altered and then deposited or cashed, according to BSA reporting. The payee line was the most frequently altered section, followed by the amount, which is typically made higher than the intended amount. Perpetrators also forged signatures and altered issuer information, which often requires washing the checks first. If a stolen check is not altered or directly deposited, criminals may use it as a template to create counterfeit checks, which was the second most frequently observed behavior. If counterfeit checks are not identified during the negotiation process, losses resulting from that initial stolen check can be significantly higher.

- Some perpetrators do not alter any information on the check and simply sign the back and attempt to negotiate it, though this occurred least frequently. In some instances, perpetrators forged the intended recipient's signature and other times they simply signed their own name or applied an indecipherable signature and attempted to deposit it.
- Other times, perpetrators opened a new account at a financial institution that had either the same name as the intended recipient or a nearly identical name and deposited the check. These new accounts were typically opened online with fraudulent or stolen identification information, according to BSA filings.

Check Manipulation Methodologies Range in Sophistication

BSA reporting indicated several methodologies used to alter, counterfeit, or fraudulently sign checks that ranged in sophistication, demonstrating that perpetrators' capabilities are expansive. Some opted for speed and ease, while others took extra effort to disguise their activity and increase the likelihood of successful negotiation. More organized check cashing rings often appeared

16. See 31 CFR 1022.320. Check cashers are required to file Currency Transaction Reports (CTRs) and other applicable BSA forms.

17. The \$0 reports and those with no amount reported were left in the dataset of this report because of how different filers reported their amounts. If no money was transferred, some filers reported the suspicious activity amount as \$0 while others included the amount that was intended to be transferred. There were also BSA reports that included both successful and unsuccessful transactions as part of the suspicious activity amount.

FINANCIAL TREND ANALYSIS

to combine methodologies to maximize their chances of success.¹⁸ The levels of sophistication identified below were broken into three general categories (unsophisticated, moderately sophisticated, and sophisticated) based on which methods take the most time, expertise, and precision to successfully execute. While some methods are relatively simple, others that are more difficult require check washing chemicals and technological expertise. Below is a brief description of identified methodologies—categorized by level of sophistication—which all occurred after a check was stolen from the mail:

Unsophisticated Methodologies

- **Fraudulently endorsing a check without modifying any information on the check:** This involved someone signing their name on the back of a stolen check and attempting to deposit it.
- **Altering the payee or dollar amount without washing the check:** Some perpetrators crossed out the payee and added their own name or changed certain letters or numbers to change the payee and/or amount. Others used white out to alter the information.
- **Third-party payments¹⁹ with no check modifications:** Instead of modifying a check, criminals attempted making it appear as though the intended payee signed it over to them and attempted negotiating the check.

Moderately Sophisticated Methodologies

- ✓ • **Check washing:** Perpetrators wash check information using available chemicals to remove original ink and replace it with new information.
- ✓ • **Selling information from a stolen check online:** Some criminals attempted monetizing the check beyond its original amount by selling the check on dark web marketplaces or online forums, according to BSA reports and open-source research.²⁰
- ✓ • **Using compromised check information to create counterfeit checks:** Criminals took stolen checks and used them as a framework to create counterfeit checks with the victim's banking information. Some criminals used more sophisticated technology to make high-quality counterfeit checks.
- ✓ • **Stealing newly ordered checks from the mail:** Some criminals stole newly ordered blank checks from the mail, forged the rightful account holder's signature, and then issued the checks to themselves or others.

18. See United States Attorney's Office, Northern District of Georgia Press Release, "Fifteen Defendants Sentenced in Stolen U.S. Treasury Check Ring," 18 December 2018, <https://www.justice.gov/usao-ndga/pr/fifteen-defendants-sentenced-stolen-us-treasury-check-ring>; State of California Department of Justice Press Release, "Attorney General Bonta Announces 56 Arrests in \$5 Million Postal Theft and Fraud Operation," 7 October 2022, <https://oag.ca.gov/news/press-releases/attorney-general-bonta-announces-56-arrests-5-million-postal-theft-and-fraud>.

19. A third-party check is a check in which the original payee has both endorsed the check and assigned it to a new payee, allowing that person to deposit or cash it. Financial institutions are not required to accept third party checks.

20. See Ron Lieber, "Stolen Checks are for Sale Online. We Called Some of the Victims," *The New York Times*, 20 December 2023, <https://www.nytimes.com/2023/12/09/business/stolen-checks-telegram.html>.

FINANCIAL TREND ANALYSIS

Sophisticated Methodologies

- **New account fraud:** New account fraud involved criminals opening new accounts, typically online, specifically designed to negotiate stolen checks.²¹ This most frequently occurred when stolen checks were made out to businesses. Some criminals opened accounts either in the name of the payee or a name that is nearly identical. The company that opened the account may not actually exist and may use a fraudulent address during the account opening process. Perpetrators may open these accounts using compromised identifying information or synthetic IDs comprising of information from several people.
- **Mail theft-related check fraud as part of a larger scam, mostly romance and employment scams:** In these cases, scammers engaged victims in a scam and convinced them to negotiate a check and then send the funds elsewhere, using the victims as money mules to move stolen funds.
- **Insider involvement:** Sophisticated operations have enlisted insider assistance at financial institutions or the USPS.²² In one case, federal prosecutors charged a USPS employee with stealing more than \$1.6 million in checks from the U.S. mail, altering the checks, and depositing them into his own account.²³

Perpetrators Try to Avoid Interaction with Bank Personnel

BSA reporting reflects that perpetrators appear to prefer depositing checks via methods that avoid in-person contact with depository institution personnel.²⁴ This eliminates a hurdle to negotiating the checks in person, as bank officials could potentially detect the fraudulent check or become suspicious of the person depositing the check, which could hinder the scheme.

- Deposits at ATMs or via RDC were the preferred method of deposit, according to BSA reports. While both allow depositors to avoid bank personnel, RDC ensures that no one from the receiving bank physically handles the check. Financial institutions noted that poorly made counterfeit checks are often made using incorrect check stock, and security features according to BSA reporting and open-source information.²⁵
- Perpetrators of new account fraud often opened their accounts online, using fraudulent identifying information or a money mule to open the account, according to BSA reporting.

-
21. New account fraud refers to fraud in newly opened accounts shortly after opening. Often, these accounts appear to be opened solely to facilitate fraud or process fraud-related payments.
 22. See United States Attorney's Office, Central District of California Press Release, "Orange County Man Pleads Guilty to \$1.2 Million Check Fraud Scheme He Promoted on Social Media," 25 May 2023, <https://www.justice.gov/usao-cdca/pr/orange-county-man-pleads-guilty-12-million-check-fraud-scheme-he-promoted-social-media>.
 23. See United States Attorney's Office, District of Columbia Press Release, "Former Postal Worker Charged with Stealing Checks from the U.S. Mail," 22 September 2023, <https://www.justice.gov/usao-dc/pr/former-postal-worker-charged-stealing-checks-us-mail>.
 24. For this report, depository institutions consist of both banks and credit unions.
 25. See Georgia Department of Banking and Finance, "Check Fraud/Counterfeit Checks," <https://dbf.georgia.gov/check-fraud-counterfeit-checks>.

Mail Theft-Related Check Fraud Affects Communities Across the United States

Financial institutions reported transactional activity or BSA filing subjects linked to every U.S. state, Washington, D.C., and Puerto Rico. While every state has been affected, populous states with large urban areas have reported more incidents. See below for additional information regarding locations of subjects identified in BSA reports. Based on a review of the BSA reports within the dataset, filers completed this field where subject location could be identified. However, the subject may not be known or their information may not be available and/or reported in all instances.

Top Five States by BSA Report Subjects (Count and per 100,000 Residents by Subject State)

Count of Subjects per State	BSA Report Subjects per 100,000 Residents
New York: 1,702	Alabama: 13.992
California: 1,458	Georgia: 10.838
Florida: 1,423	Washington, D.C.: 9.572
Georgia: 1,161	New York: 8.425
Texas: 1,007	New Jersey: 7.579

See below for additional information regarding locations of check deposit and cashing activity. As with the subject information, filers completed this field where a branch location could be identified, but this information is not always available and/or reported, including where the reported activity was conducted entirely online:

Top Five States by Branch Location Activity (Branch Location BSA Report Count and Branch Location Count per 100,000 Residents)

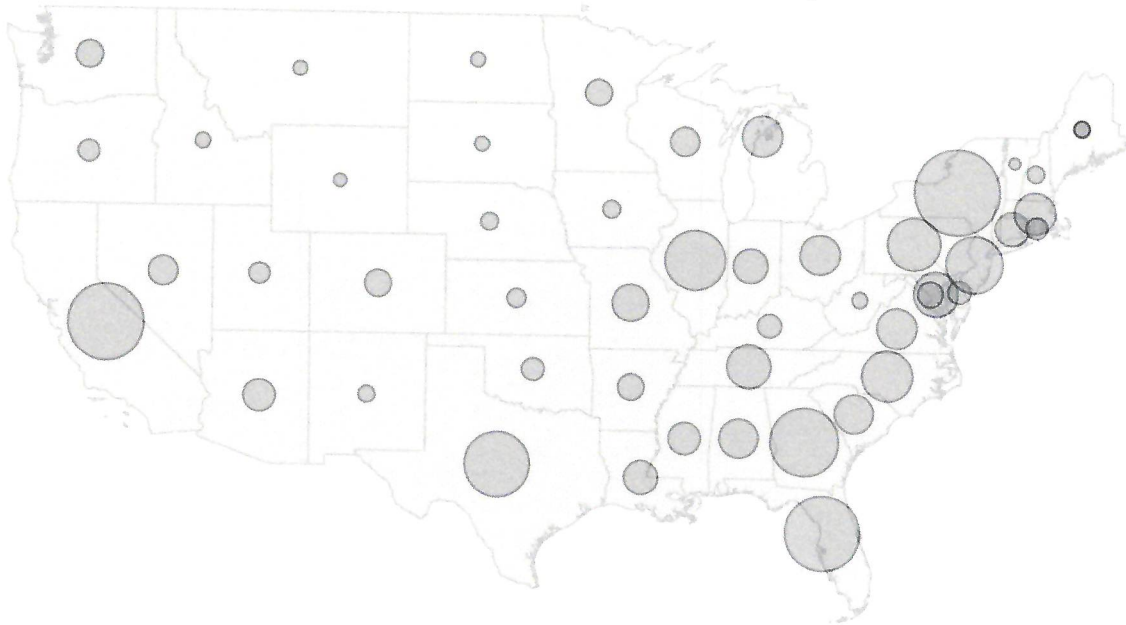
Branch Location Count	Branch Location Counts per 100,000 Residents
New York: 1,037	Washington, D.C.: 6.816
California: 745	New York: 5.133
Florida: 466	New Jersey: 4.285
New Jersey: 398	Maryland: 3.610
Illinois: 375	Delaware: 3.536

The information in this report is based on mail theft-related check fraud information obtained from analysis of BSA data, and open-source publications, as well as insights from law enforcement and other partners. FinCEN welcomes feedback on this report, particularly from financial institutions. Please submit feedback to the FinCEN Regulatory Support Section at frc@fincen.gov.

FINANCIAL TREND ANALYSIS

Appendix A: BSA Report Subjects and Branch Location Activity by State

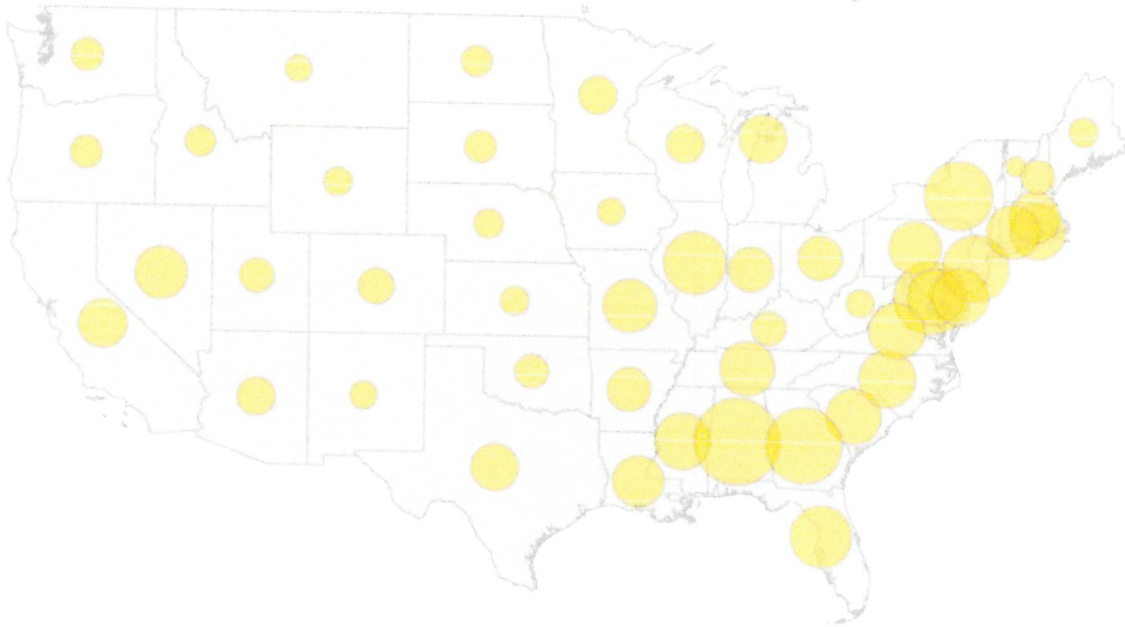
Map 1: States by Count of BSA Report Subjects



State	Subjects Count	State	Subjects Count	State	Subjects Count
AK	7	KY	69	NY	1,702
AL	703	LA	189	OH	336
AR	87	MA	308	OK	61
AZ	163	MD	345	OR	55
CA	1,458	ME	13	PA	585
CO	100	MI	372	RI	58
CT	175	MN	109	SC	265
DC	66	MO	287	SD	11
DE	56	MS	156	TN	347
FL	1,423	MT	8	TX	1,007
GA	1,161	NC	565	UT	51
HI	7	ND	9	VA	469
IA	24	NE	20	VT	2
ID	20	NH	21	WA	96
IL	894	NJ	704	WI	119
IN	204	NM	17	WV	16
KS	25	NV	144	WY	5

FINANCIAL TREND ANALYSIS

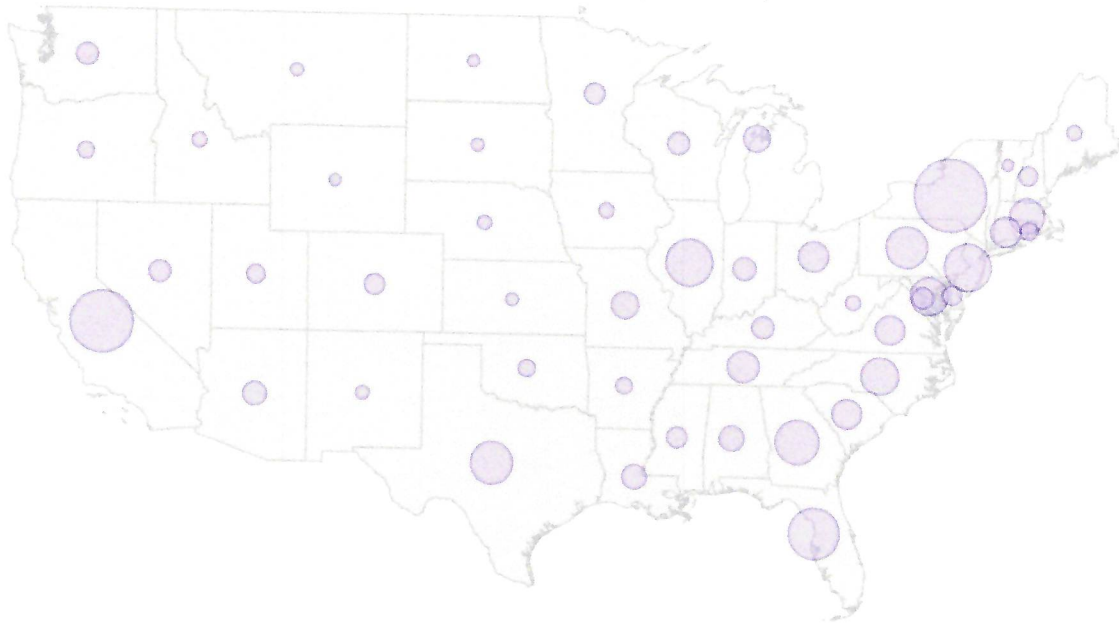
Map 2: BSA Report Subjects per 100,000 Residents by State



State	Subjects Per 100,000	State	Subjects Per 100,000	State	Subjects Per 100,000
AK	0.954	KY	1.531	NY	8.425
AL	13.992	LA	4.058	OH	2.848
AR	2.889	MA	4.381	OK	1.541
AZ	2.279	MD	5.585	OR	1.298
CA	3.688	ME	0.954	PA	4.499
CO	1.732	MI	3.691	RI	5.285
CT	4.853	MN	1.910	SC	5.177
DC	9.572	MO	4.663	SD	1.241
DE	5.657	MS	5.268	TN	5.021
FL	6.607	MT	0.738	TX	3.455
GA	10.838	NC	5.412	UT	1.559
HI	0.481	ND	1.155	VA	5.434
IA	0.752	NE	1.020	VT	0.311
ID	1.087	NH	1.524	WA	1.246
IL	6.978	NJ	7.579	WI	2.019
IN	3.006	NM	0.803	WV	0.892
KS	0.851	NV	4.638	WY	0.867

FINANCIAL TREND ANALYSIS

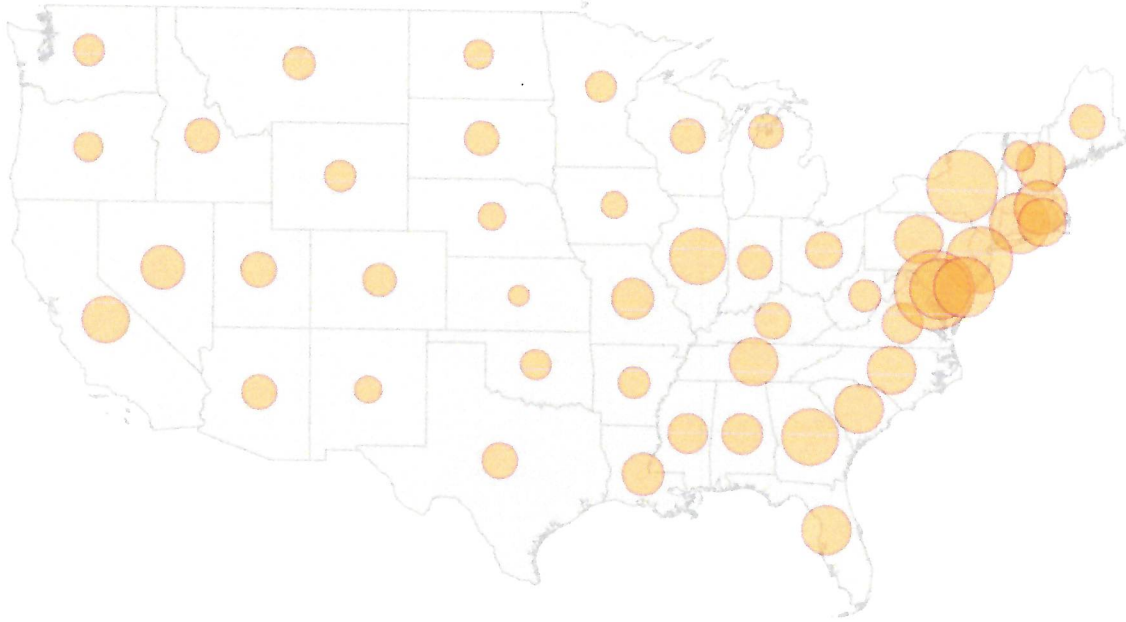
Map 3: Branch Location Activity by BSA Report Count



State	Branch Count	State	Branch Count	State	Branch Count
AK	25	KY	46	NY	1,037
AL	68	LA	68	OH	126
AR	21	MA	181	OK	25
AZ	63	MD	223	OR	24
CA	745	ME	11	PA	281
CO	43	MI	93	RI	23
CT	126	MN	37	SC	111
DC	47	MO	89	SD	8
DE	35	MS	38	TN	147
FL	466	MT	8	TX	272
GA	322	NC	220	UT	29
HI	1	ND	4	VA	126
IA	12	NE	10	VT	4
ID	16	NH	30	WA	47
IL	375	NJ	398	WI	51
IN	61	NM	10	WV	13
KS	6	NV	49	WY	4

FINANCIAL TREND ANALYSIS

Map 4: BSA Report Branch Location Activity per 100,000 Residents



State	Branches Per 100,000	State	Branches Per 100,000	State	Branches Per 100,000
AK	3.409	KY	1.021	NY	5.133
AL	1.353	LA	1.460	OH	1.068
AR	0.697	MA	2.575	OK	0.631
AZ	0.881	MD	3.610	OR	0.566
CA	1.884	ME	0.807	PA	2.161
CO	0.745	MI	0.923	RI	2.096
CT	3.494	MN	0.648	SC	2.169
DC	6.816	MO	1.446	SD	0.902
DE	3.536	MS	1.283	TN	2.127
FL	2.164	MT	0.738	TX	0.933
GA	3.006	NC	2.107	UT	0.886
HI	0.069	ND	0.513	VA	1.460
IA	0.376	NE	0.510	VT	0.622
ID	0.870	NH	2.178	WA	0.610
IL	2.927	NJ	4.285	WI	0.865
IN	0.899	NM	0.472	WV	0.725
KS	0.204	NV	1.578	WY	0.693