Check Fraud Statistics: Fraudulent Checks Remain a Significant Threat in 2025 and Beyond

Checks. They just won't go out of style. Despite ongoing efforts by financial institutions, regulators, and law enforcement, **check fraud** remains a persistent and evolving threat. Although fewer people and businesses are relying on checks in day-to-day transactions, fraudsters continue to target this method for its potential rewards. In this dive into **check fraud statistics** for 2022, 2023, and 2024, we explore how fraud schemes have evolved, the latest fraud stories making headlines, and the steps banks and credit unions can take to protect themselves and their customers.

Paper checks may seem like an outdated payment method, especially with the rise of digital payments and ACH transactions, but they still account for a large portion of business-to-business (B2B) transactions. In fact, the American Bankers Association (ABA) reported that, even in 2023, **33% of B2B payments** were made via check. The reliance on paper checks continues to make this payment method an attractive target for fraudsters who capitalize on both traditional and advanced fraudulent techniques.

Fraud continues to evolve, and the latest check fraud statistics reflect that troubling growth. Despite advancements in fraud prevention strategies across the financial sector, new vulnerabilities are being exploited at an alarming rate.

2022: The Federal Trade Commission (FTC) reported a significant spike in check fraud throughout 2022, driven largely by pandemic-related scams. Criminals took advantage of unemployment programs and government benefits, using checks to defraud both businesses and individuals. Losses tied to check fraud surpassed $24 billion, highlighting a growing trend as fraudsters increasingly turned to check-based schemes.

2023: The Association for Financial Professionals (AFP) found that 47% of organizations experienced fraud involving paper checks in 2023, a modest rise from previous years. Remote deposit capture (RDC) fraud, where the same check is deposited multiple times, played a major role in these incidents. Identity theft linked to check fraud also led to over $1.3 billion in losses for banks and credit unions.

2023 Global Check Fraud Impact: Nasdaq's Global Financial Crime Report revealed that global check fraud losses hit $26.6 billion in 2023, with 80% of those losses occurring in the Americas.

2023 Mail Theft Spike: FinCEN's Financial Trend Analysis uncovered 15,417 BSA reports citing mail theft-related check fraud in the U.S. during a six-month period in 2023, representing over $688 million in suspicious activity.

2024 Outlook: Projections for 2024 suggest that check fraud could grow even more sophisticated. The Department of Treasury's National Money Laundering Risk Assessment emphasizes the rising threat of mail theft-related check fraud. With synthetic identity fraud and business email compromise (BEC) tactics on the rise, industry leaders estimate that check fraud losses could reach $30 billion if these tactics remain unchecked—especially as more businesses transition to digital banking environments.

Check Fraud in the News

Recent cases of check fraud highlight just how creative and organized criminals have become, using technology and social engineering to execute their schemes. Below are some real-world examples of check fraud in action:

1. **New York's "Check Washing" Scandal (2023)**: In mid-2023, a sophisticated check-washing ring was dismantled in New York. This criminal network stole checks from mailboxes and altered them using chemical solutions, a process known as "check washing." They then rewrote the checks to direct funds to their accounts, resulting in **millions of dollars in losses** for local businesses and individuals.
2. **San Antonio Fraud Ring (2023)**: In May 2023, a multi-state check fraud operation was uncovered in San Antonio, Texas. The fraudsters used **synthetic identities** to open bank accounts and deposit counterfeit checks. These criminals exploited the weaknesses in remote deposit capture (RDC) systems, successfully cashing duplicate checks worth over **$2.5 million**. The case underscores the growing danger of synthetic identity fraud in the financial sector.
3. **PPP Check Fraud Scheme (2022)**: During the height of the COVID-19 pandemic, the **Paycheck Protection Program (PPP)** became a hotbed for check fraud. Fraudsters used fake businesses to apply for relief funds and then cashed counterfeit checks through a combination of RDC and in-person deposits. This nationwide scam defrauded the government of **millions in taxpayer dollars**, with many perpetrators still at large. This type of scam, where relief funds are subject to check fraud is a continual pattern, so hurricane victims of Helene and Milton should be on the lookout.

How Check Fraud Schemes Have Evolved: New Tactics for an Old Crime

Check fraud tactics have evolved since the early days of counterfeiting. Criminals are constantly finding new ways to exploit both traditional paper checks and the emerging digital check landscape. As banks and credit unions adopt remote and mobile deposit solutions, fraudsters are adapting right alongside them.

- **Counterfeit Checks**: Advances in printing technology have made it easier for criminals to produce nearly flawless counterfeit checks. Using legitimate bank routing numbers and account information, these counterfeit checks can bypass basic fraud detection systems and result in substantial financial losses for the recipients.
- **Remote Deposit Capture (RDC) Fraud**: With RDC, consumers can deposit checks by taking a photo with their phone and uploading it to their bank. While this innovation has been a game-changer for convenience, it has also created an opportunity for fraud. Criminals frequently use RDC to commit **double presentment** fraud, where the same check is deposited multiple times, sometimes across different financial institutions. In 2023, RDC fraud accounted for **$400 million in losses**, and experts warn this figure could rise in 2024.
- **Synthetic Identity Fraud**: By combining real and fictitious information, criminals create synthetic identities that pass as legitimate. They use these fake personas to open bank accounts, deposit fraudulent checks, and withdraw funds. Synthetic identity fraud has grown **28%** year over year since 2022, according to **CU Times**, making it one of the fastest-growing types of financial fraud.

Preventing Check Fraud: Best Practices for Financial Institutions

Financial institutions are the first line of defense against **check fraud**. With fraudsters employing increasingly sophisticated techniques, banks and credit unions must step up their efforts to protect themselves and their customers. Here are some best practices that can make a difference:

- **Fraud Detection Software**: Implementing advanced fraud detection tools is critical. Solutions like **check verification platforms** can analyze transactions in real-time, flagging suspicious activity before funds are lost.
- **Enhanced Employee Training**: Banks and credit unions should regularly train staff on the latest fraud trends and red flags to watch for, such as unusual check activity, mismatched routing numbers, or forged signatures. Empowering front and back office employees with the knowledge to spot fraud early is key to preventing major losses.
- **Account Holder Education**: Financial institutions should engage in proactive outreach to their account holders, informing them about the risks of check fraud and

how to avoid becoming victims. Programs that teach account holders about spotting counterfeit checks, avoiding phishing scams, and understanding the risks of RDC can significantly reduce fraud.

Regulatory Measures and the Role of Government Agencies

Regulatory agencies have been ramping up their efforts to combat check fraud, with new guidelines and requirements being introduced in 2023. The **Office of the Comptroller of the Currency (OCC)** and the **Consumer Financial Protection Bureau (CFPB)** have issued new directives requiring financial institutions to strengthen their **KYC (Know Your Customer)** protocols and enhance reporting mechanisms for suspicious activity.

Moreover, industry groups like the **American Bankers Association (ABA)** and the **National Credit Union Association (NCUA)** have been pushing for more data-sharing initiatives between banks and credit unions to help stop fraudsters before they strike. These initiatives are expected to reduce check fraud losses by encouraging greater cooperation among financial institutions.

Future Outlook: What to Expect in 2024 and Beyond

As we move further into 2024, the fight against check fraud is expected to become more intense. Fraudsters are becoming more innovative, leveraging new technologies and refining their techniques. In particular, the growth of synthetic identity fraud, combined with increasingly sophisticated phishing and social engineering tactics, poses a major challenge for the financial industry.

Despite these challenges, the outlook remains optimistic. Banks and credit unions are investing in better fraud detection systems, stronger authentication protocols, and continuous customer education programs. With the right strategies in place, financial institutions can turn the tide against check fraud and protect both their assets and their customers.

Check Fraud FAQs

How much did check fraud cost the financial industry in 2023?

In 2023, check fraud resulted in **over $1.3 billion** in losses for financial institutions across the United States, according to reports from the **American Bankers Association (ABA)**. This significant figure includes fraudulent activities such as counterfeit checks, altered checks, and remote deposit capture (RDC) fraud. Despite the decrease in check usage for personal transactions, check fraud remains a costly problem for businesses and banks, with over **47% of organizations** reporting fraud incidents involving checks during the year.

What is synthetic identity fraud, and how does it relate to check fraud?

Synthetic identity fraud involves creating a fictitious identity by combining real information—such as a Social Security number or address—with fabricated details. Criminals use these synthetic identities to open bank accounts, apply for loans, and deposit counterfeit checks. Once the account appears legitimate, fraudsters cash fraudulent checks or commit unauthorized withdrawals. This type of fraud has become increasingly tied to check fraud as criminals use fake identities to deposit or cash checks without immediate detection. In 2023 alone, synthetic identity fraud rose by **28%**, contributing to mounting losses in the financial industry.

Why has check fraud continued to rise even with the decline in check usage?

While the use of paper checks has declined over recent years, especially in consumer transactions, **check fraud continues to rise** due to its prevalence in **B2B transactions** and its susceptibility to exploitation. Checks still account for a significant percentage of business payments, making them a lucrative target for fraudsters. Additionally, new technologies, such as remote deposit capture (RDC), have introduced vulnerabilities that criminals are exploiting, including depositing the same check multiple times across different channels. The ease with which criminals can produce counterfeit checks using sophisticated printing techniques also contributes to the resilience of check fraud.

How do banks and credit unions detect RDC fraud?

Banks and credit unions utilize a variety of technologies to detect **remote deposit capture (RDC) fraud**, including **fraud detection software** that analyzes deposit patterns and flags suspicious transactions. These systems use Consortium Intelligence™, artificial intelligence and machine learning to identify anomalies, such as duplicate check deposits or inconsistencies in customer behavior. Financial institutions also rely on cross-channel verification, which involves checking whether a check has already been deposited through another method (e.g., at a physical branch). Regular audits and real-time monitoring of RDC deposits help catch fraudulent activities before funds are lost.

What can account holders do to protect themselves from check fraud?

- **Safeguard personal information**: Avoid sharing sensitive information like bank account and routing numbers unless absolutely necessary.
- **Monitor bank accounts regularly**: Keep a close eye on bank account statements and report any unauthorized transactions immediately. This is very easy in the world of mobile banking apps.
- **Use secure methods of mailing checks**: When mailing checks, consider using secure mailing options, such as certified mail, and avoid leaving checks in unsecured mailboxes.
- **Be cautious with unsolicited checks**: Always verify the legitimacy of checks received from unfamiliar sources, especially those that seem too good to be true.
- **Educate yourself on common scams**: Be aware of fraud schemes involving overpayment, sweepstakes, or job offers, where fraudsters send fake checks and ask for money in return.

How are regulators working to curb check fraud in and 2024 and into 2025?

In response to the growing threat of **check fraud**, regulators such as the **Office of the Comptroller of the Currency (OCC)** and the **Consumer Financial Protection Bureau (CFPB)** have introduced stricter guidelines for financial institutions. These guidelines include enhanced **KYC (Know Your Customer)** protocols to verify account holder identities more thoroughly and mandatory **reporting of suspicious activities** related to check deposits. In 2023, regulators also focused on improving the security of remote deposit capture (RDC) systems by recommending stronger fraud detection technology and enhanced customer authentication methods. Additionally, industry organizations like

the **American Bankers Association (ABA)** have been advocating for greater data-sharing between banks to detect and prevent fraud more effectively. Looking ahead, these efforts are expected to expand, with a focus on new and emerging check fraud tactics.