Unit21

# The Rising Tide of Check Fraud:

## How Banks and Credit Unions Can Fight Back with Advanced Technology

# Contents


Introduction.....3→

The Rise of Check Fraud.....3→

Types of Check Fraud.....5→

Minimizing Liability.....11→

The Two Sides of Check Fraud.....12→

Cost and Challenge of Catching Check Fraud.....13→

Rise of the Dark Web and Mail Theft.....14→

Hopes, Fears, and Wishes.....16→

Unit21 Solution.....17→

The Role of AI.....19→

One Stop Shop.....20→

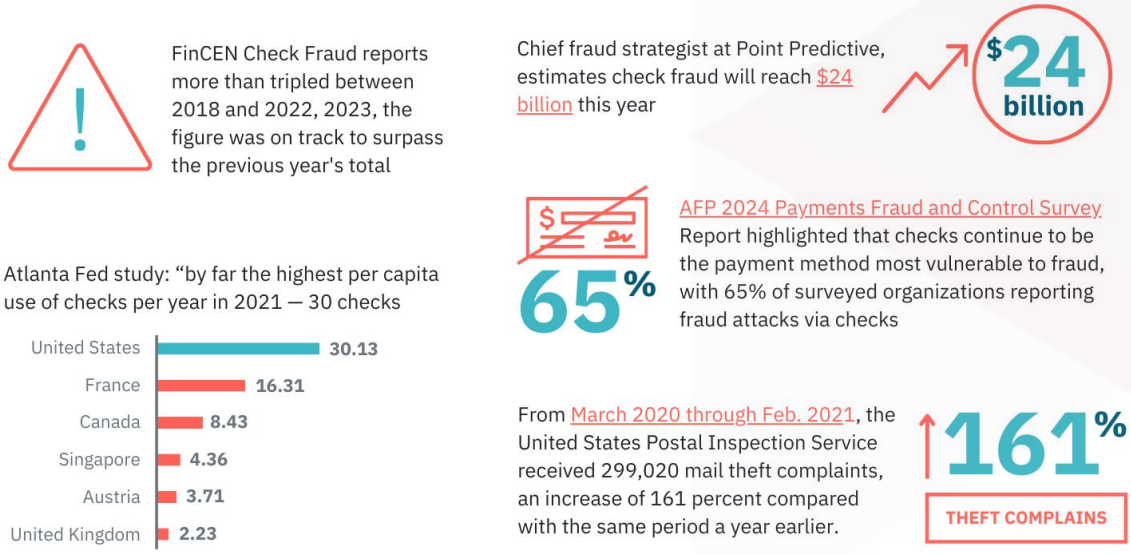
# Introduction

Banks and credit unions are suffering increased check fraud losses due to remote deposit exploits, heightened scam attempts, and a spike in counterfeiting, alteration, and mail theft. Currently, banks depend solely on reactive and retroactive ways of verifying check fraud through visual check comparison and human verification. This requires manual effort and increases the room for human error.

This whitepaper examines the prevalence of check fraud across financial institutions, the reasons behind its recent surge, the ongoing challenges institutions face in prevention and detection, and Unit21's comprehensive solution to combat this growing trend.

## The Rise of Check Fraud

The use of checks continues a downward trend, but checks are not going away any time soon. In fact, according to the 2024 AFP Payments Fraud and Control Survey Report, 70% of respondents indicated they had no plans to eliminate check usage by 2026. Although the number of checks being written continues to decrease, check fraud continues to rise. Checks remain the payment method most susceptible to fraud. [1]




[1] **"2024 AFP Payments Fraud and Control Survey Report", Association for Financial Professionals, www.afponline.org.**

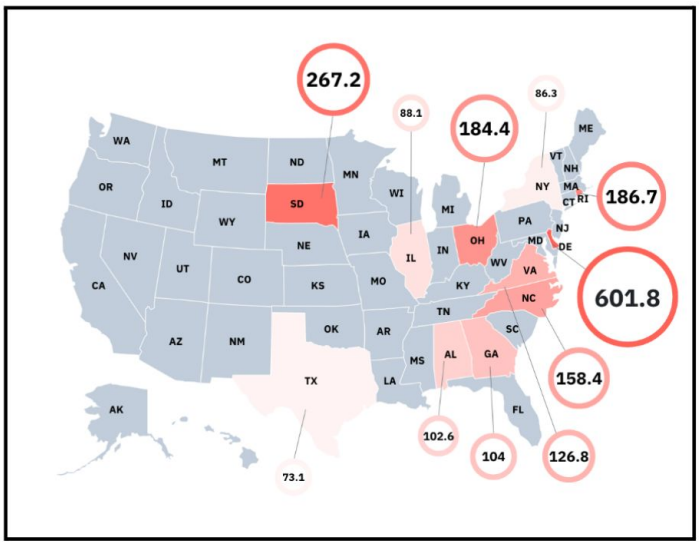
Why the surge in recent years? As financial institutions and businesses invest more in technology, including machine learning models, it poses additional challenges to fraudsters. In fact, 71% of financial institutions use AI/ML against fraud. [2] Checks are rather low-tech in comparison to wires and ACH. The lack of digital information means that financial institutions must take an analog paper check and turn it into something digital. This makes it difficult for financial institutions to write custom rules and logic to detect fraudulent checks. The lack of digital information, along with multiple deposit methods, grassroots crime through social media channels, and increased mail theft, makes check fraud a desirable avenue for bad actors.

According to the Financial Crime Enforcement Network (FinCEN), FIs filed more than 350,000 Suspicious Activity Reports (SARs) related to potential check fraud in 2021. That was a 23 percent increase over 2020. This upward trend continued into 2022 when the number of SARs related to check fraud reached over 680,000, nearly double the previous year's filings. [3]

[2] **PYMNTS. (December 2023). Financial Institutions Revamping Technologies to Fight Financial Crimes.**
[3] **"FinCEN Alert on Nationwide Surge in Mail Theft-Related Check Fraud Schemes Targeting the U.S. Mail", February 27, 2023, http://www.fincen.gov.**

## Where is Check Fraud the hottest? [3]

| State | SARS Filed - Check Fraud | State Population (2024) | SARS per 100,000 Residents |
|---|---|---|---|
| Delaware | 6,018 | 1,000,000 | 601.8 |
| South Dakota | 2,405 | 900,000 | 267.2 |
| Rhode Island | 1,979 | 1,060,000 | 186.7 |
| Ohio | 21,671 | 11,750,000 | 184.4 |
| North Carolina | 16,933 | 10,690,000 | 158.4 |
| Virginia | 11,003 | 8,680,000 | 126.8 |
| Georgia | 11,346 | 10,910,000 | 104 |
| Alabama | 5,048 | 4,920,000 | 102.6 |
| Illinois | 11,086 | 12,580,000 | 88.1 |
| New York | 16,983 | 19,670,000 | 86.3 |
| Texas | 21,963 | 30,030,000 | 73.1 |



# Nine types of Check Fraud

Check fraud is not a single, straightforward issue; it encompasses a variety of deceptive tactics. To fully grasp the scope of this problem and the challenges it poses for financial institutions, one must understand the different types of check fraud and the potential liabilities they create. There are many different forms that check fraud can take and sub-variations on how criminals attempt check fraud.

## 1. Paperhanging

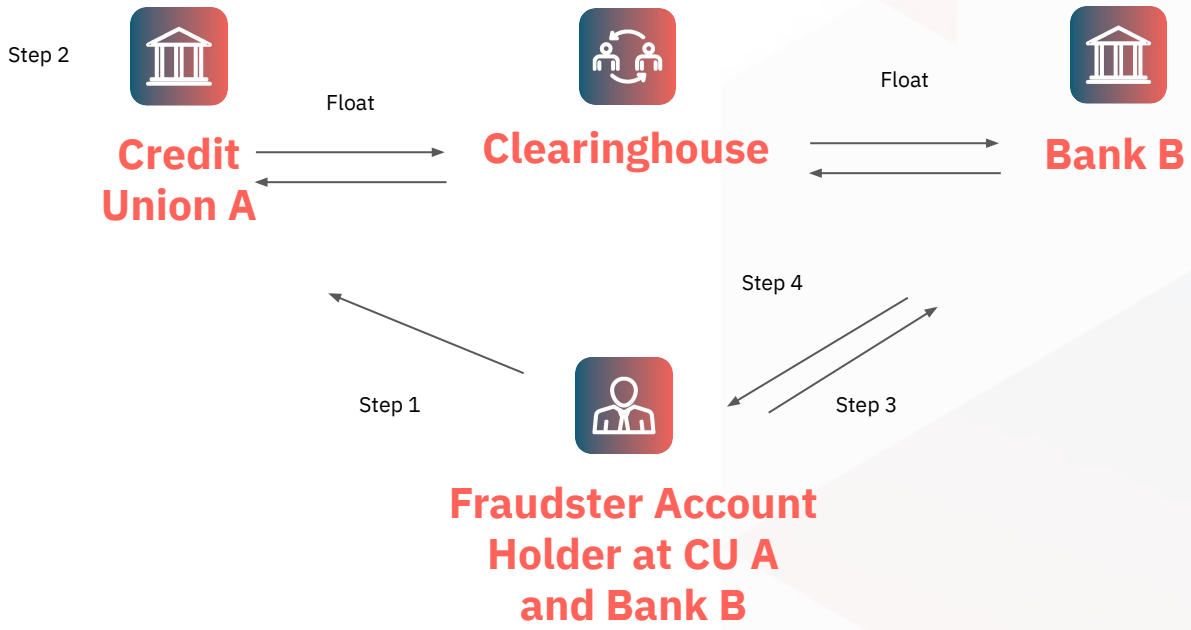
Paperhanging is a check fraud scam that exploits “the float”—the time delay between a check being deposited and cleared. A criminal will open an account at a financial institution, and then begin writing checks drawing on that account. Often, they will draw more money than they have available in the account.

The criminal will then spend the checks, or else deposit them in another account they control (and perhaps also withdraw the resulting credit as cash). Then, before the checks clear, they will utilize some other scheme to avoid accountability for the non-existent money. Fraudsters are becoming more sophisticated opening drop accounts that seem legit and lie dormant when out of the blue, they are attacked in a bust-out style fraud scheme.

# Nine types of Check Fraud

## 2. Check Kiting

Check kiting, also called check floating, is a variation of paper hanging. The criminal opens a financial account, and then begins writing checks that overdraw from that account. But during the float, instead of just disappearing, the criminal deposits money in the drawn-on account to create the illusion that it has the necessary funds to cover the checks. This money is often ill-gotten and may even be from checks that draw on accounts the criminal is depositing their original fraudulent checks into.




- **Step 1:** Fraudster deposits a check from Bank B into CU A.
- **Step 2:** CU A credits the fraudster's account.
- **Step 3:** Fraudster writes a check from CU A and deposits it into Bank B before the original check clears.
- **Step 4:** Bank B credits the fraudster's account.
- **Step 5:** Fraudster withdraws funds from Bank B before the checks clear. Both checks eventually bounce due to insufficient funds.

# Nine types of Check Fraud

## 3. Forged Endorsement

Sometimes, check fraud simply involves a criminal stealing someone else's filled-in check and then forging the payer's signature or endorsement to make the check look like it was properly authorized. They may even name themselves as the payee or alter the amount the check is for.

## 4. Check Alteration

Some fraudsters will try to erase the information on a stolen check and then write in new information to make someone else the payee or change the amount the check is worth. Sometimes they will use special chemicals to do so, which is why this is sometimes called "check washing".

More recently, fraudsters have begun the act of "check cooking" to use digital tools like AI and photoshop to alter a check image and reprint on check stock.

**Telegram Fraudster Glossary**

Terminology and slang used on social media channels like telegram:

**WASH** / wɒʃ / verb

To alter a check using chemicals to change the payee, amount, etc. *"LOOK IF YOU WANNA LEARN HOW TO WASH/SCRATCH AND COOK HMU"*

**COOK** / kʊk / verb

To create a counterfeit check. *"ANY SLIP PURCHASE COMES WITH A FREE COOK UP IF YOU NEED IT"*

# Nine types of Check Fraud

## 5. Identity Check Theft

Identity check theft is when a fraudster impersonates someone to write checks to use at the victim's expense. This may involve an account takeover, or it may involve stealing the victim's identity credentials through another method (such as phishing) and then opening an account under their name.

Either way, the criminal is now free to acquire or forge checks to either deposit into other accounts or spend like money. Meanwhile, the legitimate person behind the compromised account or identity is the one who ends up bearing the costs.

## 6. Check Counterfeiting

Criminals can sometimes create counterfeit checks that look like genuine checks, but their essential information may or may not correspond to any actual entity, bank, or account. So, the information is either for someone else's account or an account that does not actually exist.

Another counterfeiting variation is synthetic checks. Similar to synthetic IDs, this involves creating a fake check using a known legitimate bank code and account number. However, the payor information on the check does not correspond to the rightful account owner. It may not even correspond to a real entity.

# Nine types of Check Fraud

## 7. Cashier's Check

Criminals can use forged and counterfeit cashier's checks for several different check fraud scams. A common one is buying something from a marketplace by writing the seller a fake check worth more than the purchase price. The criminal's goal is to convince the seller there's a legitimate reason for overpaying (even just "by accident") and ask the seller to refund them the difference. Later, the seller finds out the check was fake and the criminal has stolen their money.

A similar counterfeit check scam involves a criminal sending a fake check to trick someone into believing they've won a lottery or been selected to receive a donation. The criminal aims to convince the victim that there were taxes, customs, or other fees associated with delivering their funds, and to send a portion of the money to cover these costs. Of course, this is just the criminal stealing money, as the victim eventually finds out the check they received was fake.

Yet another related widespread fake check scheme involves a criminal contacting a victim and offering them a job.
The fraudster sends the victim a fake check, and then asks them to use some of the money on it towards "testing" a business that sells gift cards, wire transfers, money orders, or other hard-to-trace payment assets. The criminal then disappears with the assets while the victim is left with a worthless fake check and loses the money they paid for the assets.

## 8. Treasury Check

There are multiple versions of this scam.  In one instance, a person will receive a check in the mail that appears to have been issued by the U.S. Treasury.  The accompanying letter claims the person is entitled to a grant, tax refund, or some other payment.  Sometimes the victim is instructed to deposit the check and then wire a portion back to cover taxes or other fees.  In other instances, the criminal will send the check and then contact the recipient purporting to be from the IRS, claiming that the money was sent in error and to return the funds.[5] [6] The checks look so legitimate that it has become increasingly difficult to decipher real checks versus counterfeit ones.

[5] **"Watch Out for the Latest Treausry Check Fraud Tactics [Updated for 2024], Advanced Fraud Solutions, www.advancedfraudsolutions.com**

[6] **"New Warning About Fraudulent Tax Refunds: 'These Checks Are Fake'", www.msn.com**

# Nine types of Check Fraud

## 9. Mobile Check Fraud

The modern capability of mobile device applications to deposit checks by capturing images of them is undoubtedly convenient. However, it has also opened new avenues for fraud. For instance, the potential use of editing software on these images makes checks easier than ever to forge or alter.

Another simple scheme that mobile deposit enables is double presentation. This involves a criminal capturing an image of a check to deposit it, then shortly thereafter depositing the actual physical check at an ATM or financial institution. This takes advantage of the float to deposit the check twice before the original deposit clears. The criminal may even alter the check before physically depositing it to make it more difficult to tell that it is the same check they deposited through the mobile app.

**DROP ACCOUNT** / *drɒp ə ˈkaʊnt* / noun

An account used to receive fraudulent funds. “Who wanna learn how to get into accounts and start wiring!? You’ll always need drop accounts to wire/zelle to right away”

# Minimizing Liability

In addition to the rise of check fraud and the complexities associated with its detection, financial institutions face the challenge of determining liability for losses. Check fraud can affect both the originating financial institution (known as the drawee bank or paying bank), where the check is drawn from, and the receiving financial institution (bank of first deposit or depositary bank), where the check is deposited.

When a check is presented, there are timeframes to be followed and certain warranties made by the different institutions. For the drawee bank, the Uniform Commercial Code (UCC 4-401)[7] states that it may only pay a check that is properly payable. When a check is presented, the depositary bank is tasked with identifying whether a check has been altered. The bank must also ensure there are no forged or unauthorized payee or drawee endorsements and essentially guarantees to the paying bank that the warrantor is a person entitled to the payment.

In the event a check is presented to the paying bank, and it's identified as counterfeit or contains a forged drawer's signature, the paying bank must return the item to the depositary bank before the midnight deadline under UCC 4-302[8], which is midnight on the next banking day following presentment of the check to the paying bank. There are additional time requirements that must be satisfied under Federal Reserve Regulation CC[9].

If the paying bank claims a check is altered or contains a forged payee endorsement (which the depositary bank should have caught), then the paying bank has a breach of warranty claim against the depositary bank, which can be up to three years, depending on the form of UCC adopted in the applicable state.[10]

In the 2021 case, Provident Sav. Bank vs. Focus Bank, the nuisances of these timelines and warranties are highlighted as banks continue to determine who is at fault. In this case, a customer at Provident Bank deposited a check over $150,000 drawn from a Focus Bank customer. It was after the midnight deadline that the drawer of the check alerted Focus Bank to the fraudulent check, prompting Focus Bank to return it through the Federal Reserve Bank to Provident.

[8] **https://www.law.cornell.edu/ucc/3**

[9] **https://www.federalreserve.gov/paymentsystems/regcc-about.htm**

[10] **"Back with a vengeance: The challenges of check fraud," ABA Banking Journal, bankingjournal.aba.com.**

# Liability

The two banks went back and forth, and ultimately, it came down to whether the check was altered or counterfeit. The court determined it was a counterfeit item, which meant that Focus Bank was liable since the bank did not report the counterfeit item before the midnight deadline.[11] The case reinforces the challenges financial institutions face when determining liability.

## Gaps and Challenges

Both the bank of first deposit and the paying bank are presented with a myriad of challenges. The paying bank must detect fraudulent signatures and alterations, ensuring that the signatures and other details have not been tampered with or modified. This bank must also manage stop payment requests and the enforcement of such. The bank is responsible for safeguarding customer accounts from unauthorized access and monitoring a high volume of transactions efficiently without errors. The bank is also tasked with educating customers on ways to prevent fraud on their accounts.

The bank of first deposit must verify check authenticity by confirming a check is not counterfeit prior to processing. This bank must also balance the need to make funds available to customers quickly under regulatory requirements while also preventing and detecting fraud. The depositary bank handles the financial and administrative repercussions when checks are returned unpaid and utilizes technology to detect fraudulent checks without slowing down processing times.

Currently, banks are often relying on legacy rules and human verification when determining if a check is legitimate. The manual nature of verifying signatures and calling customers or other FIs increases the chance of error and the time it takes to perform the investigation.

**Frank McKenna, Point Predictive**

"I think check fraud is going to hit $24 billion or more this year. This will be a 50% increase from the last time it was measured in 2018."

[11] **"Provident Sav. Bank v. Focus Bank", CaseText, https://casetext.com/case/provident-sav-bank-fsb-v-focus-bank.**

# Cost and Challenge of Catching Check Fraud

Fraud analysts expend significant manual effort researching possible check fraud items to determine their legitimacy. An analyst may look at things such as the length of time the customer has been with the bank or pulling up and comparing other items to look at the check stock and signature. The analyst will try to determine if the payee information matches what is on the account, if it is consistent with previous customer behavior, or if there were obvious alterations made to the check. They may even research a business account to ensure it is an active LLC. Unfortunately, many states require little to no verification to create an LLC other than a nominal fee.  Fraudsters exploit this by opening business accounts in the same, or similar name, to a payee of a stolen check in order to cash it.

In addition to the manual intensity, it is further complicated by siloed systems with data across multiple databases.  For example, an analyst must typically view customer data with the bank's core system, then image archive data is typically housed within another database, and oftentimes FIs use a fraud case management system. The analyst must use all three to research a single item. The time and effort required lead to a high false positive rate and unmanageable workload. If that's not enough, fraudsters are continually advancing their tactics, always staying one step ahead.

# Rise of the Dark Web and Mail Theft

Many have heard of the dark web, a part of the World Wide Web that is only accessible with a special browser called TOR (the Onion Router). The Dark Web is often used by bad actors to commit a plethora of crimes and sell illegal information, weapons, or drugs. It is also a convenient place to sell stolen credit card information, credentials, and checks.

Historically, banks would catch check fraud in the act upon deposit at the bank. Long before Check 21[12] and imaging of checks, tellers would sight paychecks by comparing signatures on checks to the signatures on file. Fast forward to today, and things are moving at a rapid pace. Not only are checks moved from institution to institution digitally, but catching fraud is happening long before the check is presented to the bank for deposit.

Social media and platforms like Telegram have also made it easier for criminals to obtain stolen checks, recruit for fraud rings, and create an underground supply chain. The dark web requires specialized software and knowledge on how to obtain the stolen goods. With Telegram, anyone can download the app, and with a few keywords, find stolen checks and other goods for sale. The messages are encrypted, and anonymous usernames make it next to impossible for law enforcement to track down the true messenger. Not only that, but criminals are using Telegram to actively recruit people to assist with the scams. "Walkers" are those who physically take counterfeit or altered checks into the bank for deposit.

**WALKER** */ˈwɔːkər / noun*

Someone who goes into a bank or other institution to negotiate a fraudulent check.
*"bro he asked my friend to be his walker"*

[12] **https://www.ffiec.gov/exam/check21/check21foundationdoc.htm**

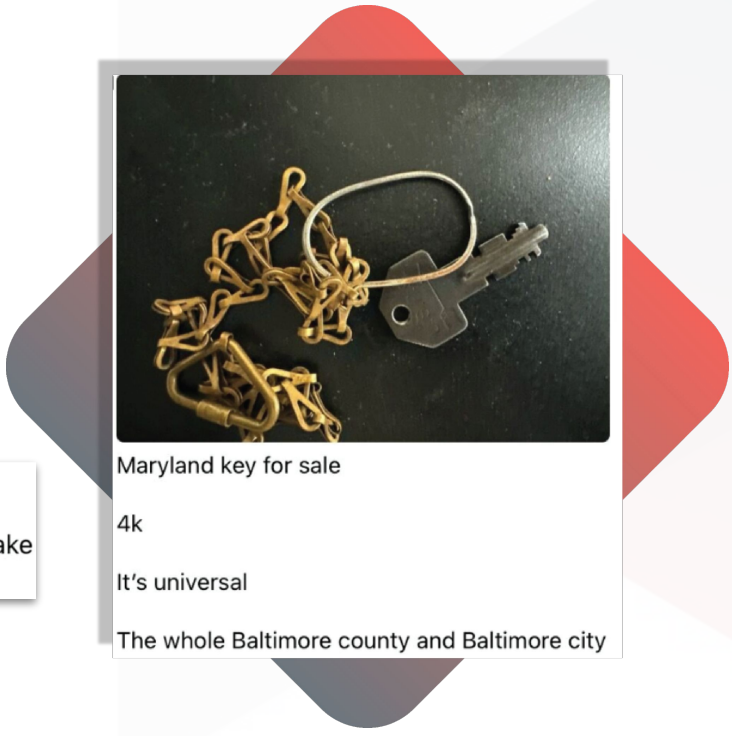
# Rise of the Dark Web and Mail Theft

Mail theft is also contributing to the rise of check fraud. In an alert issued by FinCEN, financial institutions are warned to be vigilant in identifying this type of fraud. The alert was issued in close partnership with the United States Postal Inspection Service (USPIS) and included red flags for institutions to identify mail theft-related check fraud and report such activity appropriately. The United States Postal Service delivers nearly 130 billion pieces of U.S. mail yearly to over 160 million residential and business addresses across the United States. From March 2020 through February 2021, the USPIS received 299,020 mail theft complaints, which was an increase of 161 percent compared with the same period the prior year. [13]

The rise in mail theft has further exacerbated the check fraud problem. Criminals are targeting blue boxes and other cluster units to steal checks. On social media platforms, it is not uncommon to find “arrow keys” for sale that open all mailboxes in a geolocation for more than $4,000. There have been cases of postal workers stealing checks at sorting and distribution facilities. These workers are often recruited for more than $5,000 per month as “Innys” (insiders). However, the USPIS states that most of the fraud is being committed by non-USPS employees.

**INNY** / ˈɪni / *noun*

A person inside an institution or the USPS working with the fraudster. *"gotta wells inny who got motion for that"*




[13] **“FinCEN Alert on Nationwide Surge in Mail Theft-Related Check Fraud Schemes Targeting the U.S. Mail”, February 27, 2023, www.fincen.gov.**

# Hopes, Fears, and Wishes

To some, it feels as though FIs are fighting an uphill battle. Banks and credit unions are frustrated with the high rate of check fraud, despite precautions. New solutions are often difficult to integrate with legacy solutions, and the high rate of false positives leads to customer dissatisfaction. The sheer workload and manual processes slow down response times, and often, staff turnover leads to undertrained and overwhelmed employees. There often isn't a budget for new fraud initiatives, and there is an inconsistency in fraud reporting standards.

FIs fear that financial losses will continue to increase due to sophisticated fraud schemes, which can lead to reputation damage, especially when there are high-profile fraud cases. This leads to distrust and impacts customer loyalty. FIs must also stay on top of regulatory requirements and ensure compliance. What most want is an effective, real-time fraud detection solution that seamlessly integrates with other systems. FIs want to automate routine tasks, reduce false positives, and use advanced analytics to better predict and prevent fraud without missing actual fraud.

# Unit21 Solution

Considering the entire landscape of check fraud, Unit21 has created a holistic solution: Check Fraud Investigation & Prevention, which allows agents to self-sufficiently manage how and what to flag as fraud with out-of-the-box rules without relying on engineering. With a toolkit of advanced ways to monitor and flag suspicious activity, analysts can efficiently and effectively verify checks with a holistic view of an account's historical and recent activity – and even catch check fraud on the dark web and Telegram long before an account is compromised. Unit21's solution eliminates manual effort, cuts down investigation time, and proactively flags fraud.

## The Role of Automation

Unit21 monitors the dark web, Telegram, and any other channels where stolen checks could be sold. Monitoring stolen checks by routing number allows Unit21 to find them before reaching the bank and compromising a customer's account.  Third Coast Bank was able to confirm that $50,000 in check fraud was prevented from the initial seven alerts from Unit21's monitoring.

"After turning on Unit21's check fraud rules and alerting, specifically dark web monitoring, we caught and **prevented $50,000** in potential check fraud from **just the initial 7 alerts**"

Jo Davenport. SVP Fraud Director, CFCI

THIRD COAST BANK SSB

**"2024 AFP Payments Fraud and Control Survey Report", Association for Financial Professionals, www.afponline.org.**

# Unit21 Solution

Unit21's solution contains out-of-the-box rules that can be quickly and painlessly deployed within minutes to gain a holistic view of all data. Traditional rules are simplistic, and fraudsters are quickly able to figure out thresholds and stay beneath them to avoid detection. The standard rule sets with Unit21 are far more complex. The out-of-the-box rules look at things such as serial numbers, duplicates, and whether a check matches a recent deposit. FIs can even filter on particular conditions for business accounts.

Rules can be validated and tested before going live. The "shadow mode" feature looks at the data set and provides feedback before analysts get actual alerts to determine if the rule is effective or needs additional tweaking, helping to avoid high false positive rates.


**"2024 AFP Payments Fraud and Control Survey Report", Association for Financial Professionals, www.afponline.org.**

# Unit21 Solution

## The Role of AI

The AI Agent quickly understands the data and provides clear, actionable insights for each fraud investigation. Couple that with the Check Investigation Toolkit, and this gives the user a holistic view of data. This toolkit centralizes and automates all check transactions, historical deposits, and image comparisons (including the signature on file and signature comparisons of other signatures) in one place to work investigations quickly and efficiently.  Instead of going to multiple systems to see the whole picture, analysts can view everything in one place to make an informed decision.

Unit21 also uses image analysis to look at signatures and endorsements. Analysts can compare signatures from the signature card or a driver's license and look for any alterations. As analysts mark items as fraudulent, machine learning uses that feedback loop to detect actual fraud better, reducing false positives.

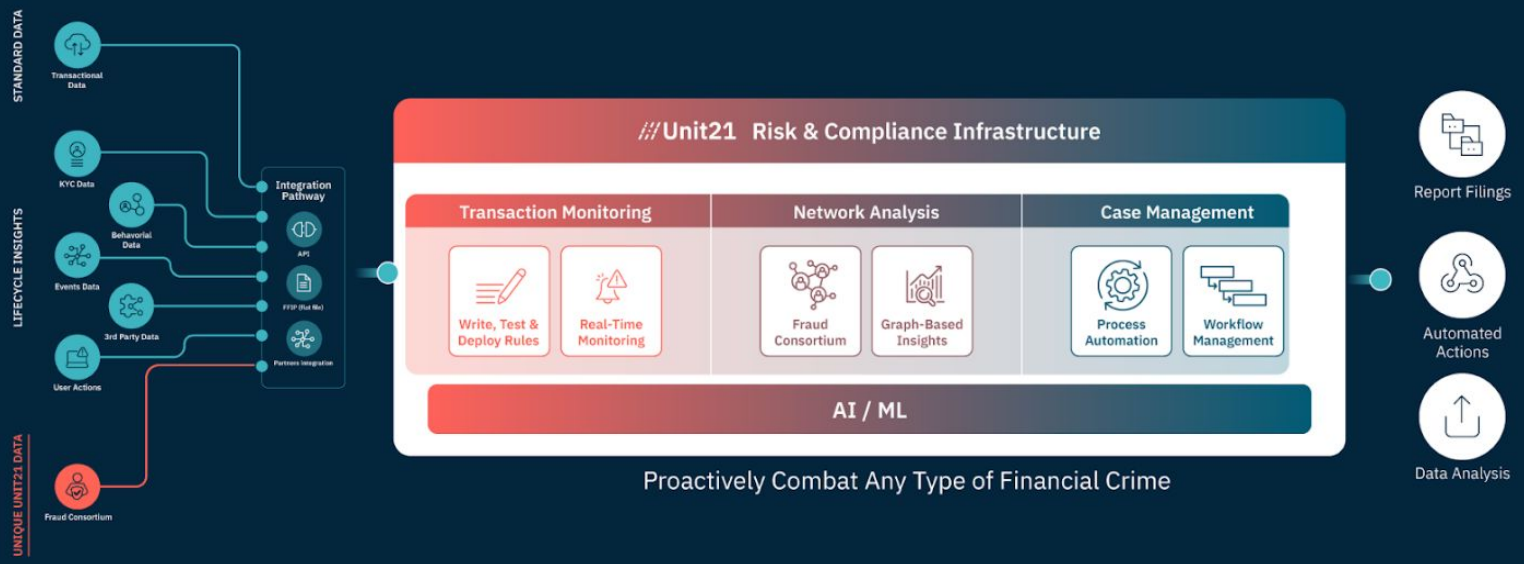

**"2024 AFP Payments Fraud and Control Survey Report", Association for Financial Professionals, www.afponline.org.**

# Unit21 Solution

## One Stop Shop – Future-Proof against Fraud, Risk and Compliance Issues

Unit21 brings together data from multiple places into one, comprehensive solution to help detect and prevent not just check fraud but much more. The platform allows all fraud and AML activity to be brought into a single pane of glass for easy de-risking and decision-making.

Hundreds of companies have chosen Unit21 because of the pre-built rules and automations that can help deploy a sophisticated risk solution in a matter of weeks. With Unit21, risk and compliance teams can create and iterate their own rules and models, without having to send them off to engineers. To add to Unit21's ease-of-use, it automates workflows and SAR filings so teams can do away with inefficiency and inaccuracy to focus on what matters most-proactively stopping fraudulent activity.




**LET US CREATE A CUSTOM DEMO INSTANCE FOR YOU**

### Unit21 2023 Impact

**$2.7T**
transactions processed annually

**35M**
users monitored with Fraud Consortium

**$4.3B**
prevented in fraud attempts

**28K**
Suspicious Activity Reports filed