REFINE
INTELLIGENCE

The Check Fraud Kill Chain

Moving from Detection to Prevention

For more information visit www.refineintelligence.com

Table of Contents

What is a ‘Kill Chain’?

The term "kill chain" traditionally originates from cybersecurity, where it describes the steps attackers take to infiltrate and exploit systems. In the context of this ebook, we are borrowing this term to analyze the sequence of actions fraudsters follow to commit check fraud. By understanding each step in this fraud kill chain, bank fraud teams can effectively mitigate the risk at various stages, from detection to prevention.

Introduction

Talking about check fraud may feel like going back in time for an industry that has already solved so many forms of online fraud. But despite the declining use of paper checks, the scale and sophistication of check fraud in the U.S. is on the rise.

$24 billion

Expected 2024 check fraud losses

In 2024, losses from check fraud are expected to reach $24 billion, according to Bank Automation News.[1]

Thomson Reuters reports that last year, 666,000 check fraud-related SARs accounted for almost 20% of all SARs filed,[2] and Datos shows check fraud to be the fastest growing type of fraud in U.S. banking.[3]

The overwhelming numbers put tremendous pressure on fraud investigation teams at banks. This ebook discusses the **liability and challenges** in fighting check fraud, and provides **best practices** for reducing check fraud losses while maintaining better engagement with customers.

Check Fraud Liability

Once a check is deposited, the collecting bank sends an image of the check to the issuing bank, which must approve it by afternoon of the next day. If the check is approved and fraud is later reported by the issuing bank's customer, liability depends on the type of fraud:

Altered Check

If the original check was deposited, but the beneficiary name was altered, usually through a chemical process called "washing," **the bank where the check was first deposited is held liable**. The rationale: the beneficiary's bank should know them really well.

...

How long have they been with the bank? Do they normally receive this amount of money? Do they normally receive checks?

Counterfeit Check

If the check is a counterfeit, and the original check is never deposited, the **originating bank is accountable for the loss**, as it should be able to identify the forgery.

...

Is the signature correct?
Are there any discrepancies related to the check's serial number?
Are there any visual deviations?
Is this a 'normal' transaction?

The current crime wave has a unique pattern that blurs the clear lines of responsibility, and has gained momentum with the mass sending of COVID-19 relief checks. Checks are physically stolen rather than counterfeited, but they are not simply altered.

Example: A check is intercepted via mail theft—either by targeting an individual's mailbox or attacking the supply chain (e.g., couriers, central mail processing centers). The check is then scanned and reproduced—either digitally for a mobile app deposit or printed for an ATM/branch deposit (with a new beneficiary).

Since the deposited item is not a doctored original but rather a fake copy, the bank of the first deposit might argue that it should not be considered an ‘altered check,’ which means they are not liable. The issuing bank might argue that it is not a forged check either, but rather the original check being manipulated and deposited, which means they are certainly not liable.

There’s a heated argument in the industry about who is really liable, but the dynamics are clear: **if fraud is reported, the issuing bank needs to handle the dispute, reimburse the customer, and attempt to recover the money from the collecting bank.**

Another thing is clear: **the issuing bank has weak signals to operate on.** Detection is challenging, and resolving alerts is even more difficult given their large volume and the saturation effect that fraud teams face.

A special case occurs if the check is drawn on the same bank in which it is deposited. In this case, just one bank is responsible for determining its validity, and these are known as 'on-us' checks.

Challenges for U.S. Banks Fighting Check Fraud

While fraud prevention teams make valiant efforts to protect the integrity of the bank’s checks, they face five key challenges:

Teams Are Overwhelmed By a Huge Volume of Alerts

Given the advanced manipulation techniques and the use of stolen checks for forgery, detection normally produces a massive amount of alerts, the vast majority of which are false positives. This high false alarm rate and elevated ‘noise’ level overwhelms fraud and business operations teams, increases human error, and diverts attention from actual fraud.

Limited Investigation Time

Fraud prevention teams have limited time to review checks before they are cleared and funds are transferred - typically just 4–5 hours. This is worsened by the daily volume of on-us and in-clearing checks, which can amount to hundreds or even thousands for larger institutions.

This urgency requires teams to be highly-efficient and accurate, but manual reviews are very technical and labor-intensive. Some fraudulent checks slip through the cracks, leading to significant financial losses.

Internal Exploitation

Processing on-us checks adds another challenge, because these checks often undergo fewer verification steps than those processed through external clearinghouses. This internal processing can create blindspots and bypass certain fraud detection mechanisms. Fraudsters exploit this by opening fake accounts in the bank from which the check is stolen, thus generating on-us situations, knowing they will encounter the scrutiny of only one bank before the check clears.

Real-Time Information Gaps

Verifying the beneficiary and authorization of a check in real-time is challenging due to the scarcity of data. Teams often rely on limited information, making it difficult to confirm whether a check is genuine and increasing the likelihood of fraudulent checks being processed.

High Fraud Costs and Operational Overhead

Besides direct customer losses, check fraud exposes banks to regulatory fines, high operational overhead, and significant customer reimbursement costs which can result in substantial financial losses. The additional resources required to investigate and resolve fraud contributes to a high operational overhead. This financial burden is increased by the potential reputational damage that can negatively impact customer trust and loyalty.

How Check Fraud Detection Works

Detecting in-clearing check fraud between the time a check is deposited and the time it clears typically leverages several capabilities:

- **Graphical analysis for signs of manipulation:** For example, subtle changes in the way the beneficiary's name is written vs. other elements on the check, signature verification, and other visual cues of forgery or digital manipulation.

- **Checking if the beneficiary has previously received payments from this account** by comparing their name with past transactions.
- **Verifying checkbook serial numbers** to see if there are duplicates or if the check number is out of sequence based on the deposit time.
- **General transaction profiling** that maps the customer's activity.
- **Dark Web monitoring** to identify stolen checks sold in marketplaces and forums.

Once a check is flagged based on these criteria, the alert does not resolve itself. It goes to an investigator who determines if the flagged checks are indeed fraudulent.

Fraud leaders often search for better detection systems to reduce false positives (FPs). Choosing, implementing, and fine-tuning check fraud detection systems can be time-consuming. Efficiency improvements may result from recalibrating and focusing on a new implementation effort rather than from superior technology. To the team's dismay, the process is typically very long. The result is often an improved, but still high, false positive rate.

Check Fraud Alert Investigation and Resolution

Given the high FP rate, a check fraud prevention program cannot stop at detection. In fact, detection is only the first step.

As mentioned, check fraud alerts do not resolve themselves. What comes next is an operational phase designed to swiftly investigate the alerts and identify the fraudulent checks. To fully prevent the fraud, the manipulated check needs to be detected, then investigated, and **correctly decided upon in a narrow window of time**—typically a few hours in the morning following the deposit.

Fraud teams aiming to improve check fraud prevention must first collect data for an effective analysis:

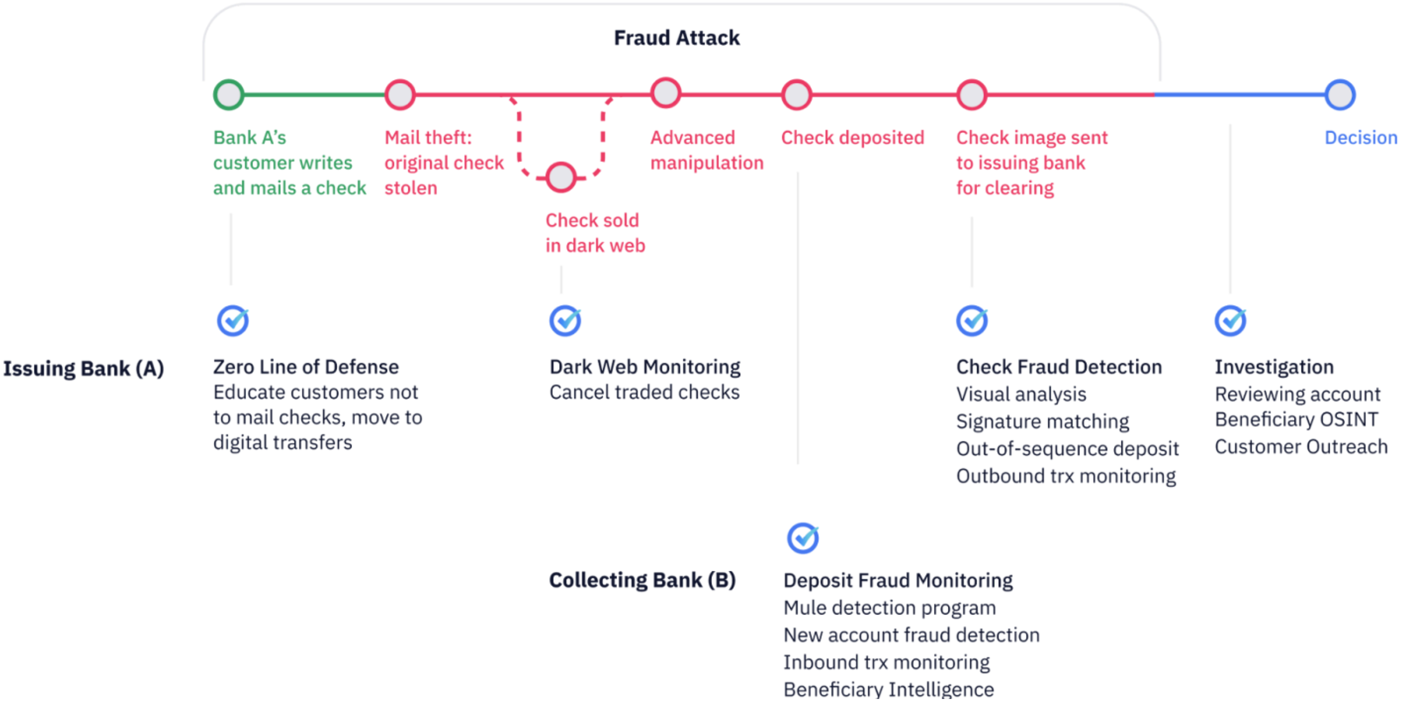
- How many fraudulent checks are deposited each day (prevented, unprevented, and reported)?
- Out of that, how many were alerted?

- Out of the alerts, how many did the team have time to investigate?
- Out of that, how many fraud cases were identified correctly and stopped vs. false positives?

The Check Fraud Kill Chain

The check fraud kill chain analyzes a fraud attack from the perspectives of both the fraudster and the bank's fraud team, illustrating a step-by-step process of the fraud and countermeasures by the bank.

Initially, a bank customer mails a check and it is stolen. The issuing bank's (A) "zero line of defense" should be customer education to use digital transfers. In many cases, checks stolen from the mail are sold in dark web marketplaces, prompting banks to use dark web monitoring tools and cancel traded checks. Fraudsters then manipulate the stolen checks by scanning and altering the information ("advanced manipulation"), making them harder to detect.



The check fraud kill chain. Source: Refine Intelligence

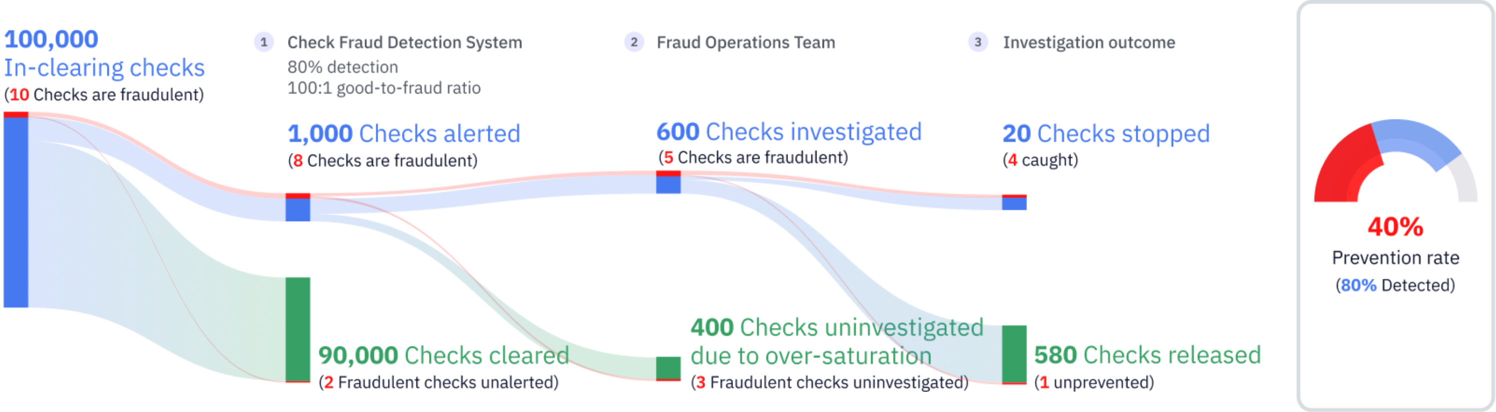
When the fraudulent check is finally deposited, the collecting bank (B) may utilize deposit fraud monitoring systems, including mule detection programs, new account fraud detection, inbound transaction monitoring, and beneficiary intelligence, to identify suspicious activity.

Finally, as the check is scanned and sent to the issuing bank for clearing, banks use check fraud detection techniques like visual analysis, signature matching, out-of-sequence deposit tracking, and outbound transaction monitoring to identify and mitigate fraud.

The Fraud Prevention Process: A Theoretical Example

Here is a theoretical scenario that can also serve as a practical framework. You can use this as a template and plug in your own numbers. For the sake of this exercise, let's consider a bank that experiences an average of 10 fraud attempts per day.

The process begins with an influx of 100,000 in-clearing checks. These checks are initially screened by an automated fraud detection system (#1 in the diagram below), which flags any check matching a set of predefined rules indicating potential fraud.


100,000
In-clearing checks
(10 Checks are fraudulent)
1 Check Fraud Detection System
80% detection
100:1 good-to-fraud ratio
1,000 Checks alerted
(8 Checks are fraudulent)
90,000 Checks cleared
(2 Fraudulent checks unalerted)
2 Fraud Operations Team
600 Checks investigated
(5 Checks are fraudulent)
400 Checks uninvestigated due to over-saturation
(3 Fraudulent checks uninvestigated)
3 Investigation outcome
20 Checks stopped
(4 caught)
580 Checks released
(1 unprevented)
40%
Prevention rate
(80% Detected)

Use your bank's data with this framework to determine where to invest in improving your check fraud workflow for improved ROI. Source: Refine Intelligence

Let's assume the system is calibrated to detect 80% of fraud at a good-to-fraud alert ratio of 100:1. This means that for every fraudulent check, the system also alerts on 100 legitimate checks. This translates to 1000 alerts per day given the 10 fraudulent checks. Consequently, 2 fraudulent checks pass through undetected and result in a fraud loss.

The team can aim for better detection at the expense of more alerts or fewer alerts at the expense of reduced detection. In our example, we chose 80% detection at roughly a 99% false positive rate. Following the initial automated screening, the fraud investigation team (#2 in the diagram above) takes over and proceeds to the manual investigation phase. The team has to review 1000 alerts with 8 fraud cases in that risk bucket. Investigators will typically have up to 10 minutes to review a case. After triage, 600 alerts are reviewed (400 are not, due to over-saturation and operational constraints), and 20 checks are stopped. We'll assume that out of the 20 stopped checks, 3 were actually fraudulent, and 17 were wrongly halted. Out of 980 alerts, 5 fraudulent checks were cleared by mistake.

The end result is that 4 out of 10 daily fraudulent checks were not cleared for deposit. The remaining 7 were cleared and resulted in a loss for the bank.

4 of 10

Daily prevented fraudulent checks in this scenario

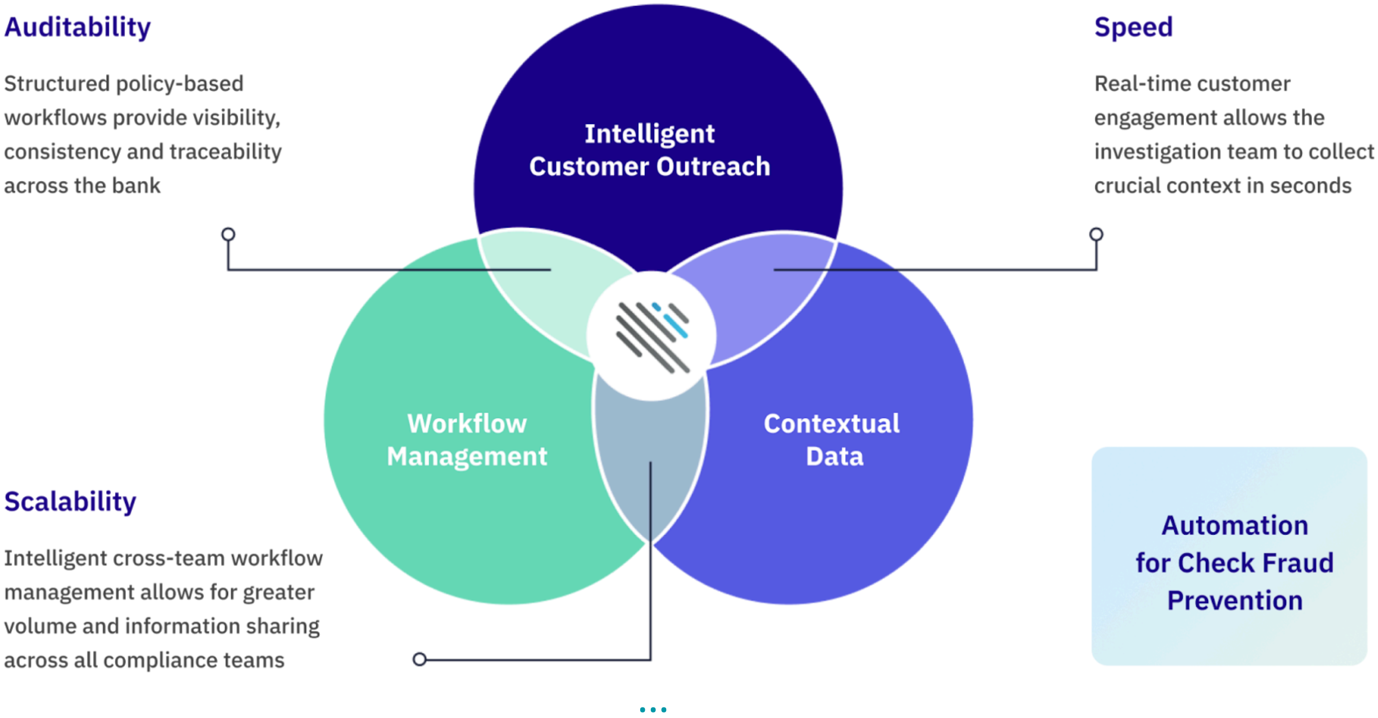
Think of the figures in the example above as placeholders. Your fraud team must collect and understand all these performance metrics, then plug them into the calculation to identify gaps and areas for improvement.

Questions the fraud team should consider when examining a sub-optimal workflow:

- Is it a detection problem?
- How are the detection rules performing?
- Is it a workload or saturation issue? If so, this means that adding more resources may lead to an improved ROI.
- Does the investigation team have enough context to resolve alerts efficiently? A significant gap between alerted checks and prevented fraud would indicate this, suggesting that the best investment is in adding automation and improving the context available to the investigation team.

Best Practices for Check Fraud Prevention

These complex challenges require trade-offs between effective fraud prevention, cost-effective operations, and customer experience. Investing in automation can significantly enhance check fraud investigations while minimizing false positives and operational overhead:



Auditability

Structured policy-based workflows provide visibility, consistency and traceability across the bank

Speed

Real-time customer engagement allows the investigation team to collect crucial context in seconds

Scalability

Intelligent cross-team workflow management allows for greater volume and information sharing across all compliance teams

Automation for Check Fraud Prevention

Best practices for check fraud prevention automation blends together high velocity RFIs, contextual data and Workflow management. Source: Refine Intelligence

Intelligent Customer Outreach

The best way to resolve an alert is by showing the check to the customer and asking whether everything, especially the beneficiary, is correct. However, chasing customers over the phone is highly unproductive, wasteful, and yields low response rates. Most banks use this method in less than 5% of alerts. The customer signal is extremely potent, but for it to be used effectively, an automated method of reaching out to customers is required. If done properly, the bank can move to a new era of high-velocity RFIs.

Banks that engage in automated customer outreach use multiple digital channels to reach the right customer, at the right time, with the right context, asking the right questions, and routing the answers to the right teams. There are several important considerations that should be taken into account:

- **Orchestration**: Use intelligent controls. Which alerts should trigger an outreach? Which specific customers should be reached? When should each notification be sent, given time zone differences?
- **Customer Segmentation**: Not all of your customers are the same. Elderly customers have different communication preferences compared to younger customers. Customers who live in rural areas or overseas will also require a certain degree of customization.
- **Reminders**: Automated reminders can boost the response rate, but you need to handle them with care. What frequency should be used? What tone of voice? When should reminders stop?
- **Usability**: Providing a positive customer experience is an absolute must. EA/B testing of each customer-facing component is of paramount importance. What context should be given, and when? What visuals should the customer view?
- **Privacy**: Customers should be approached with respect, and privacy is a key consideration. If you show any information to the customer, make sure private information is masked.
- **Utilize Analytics**: Automatically trigger and deliver RFIs, allowing your team to concentrate on more complex investigations.

Workflow Management

Banks need to implement effective 1st/2nd line workflow management to gain insights into check investigation processes, confirmed fraud vs. verified checks, and customer RFI statistics. To adopt this approach successfully, banks should follow these best practices:

- **Deploy an integrated platform:** Eliminate organizational silos and provide the 1st and 2nd line teams with a single source of truth for check fraud prevention.
- **Smart routing:** Direct tasks to the appropriate 1st or 2nd line team based on the investigation workflow and set criteria, enabling efficient task tracking with a full audit trail

and workflow automation.

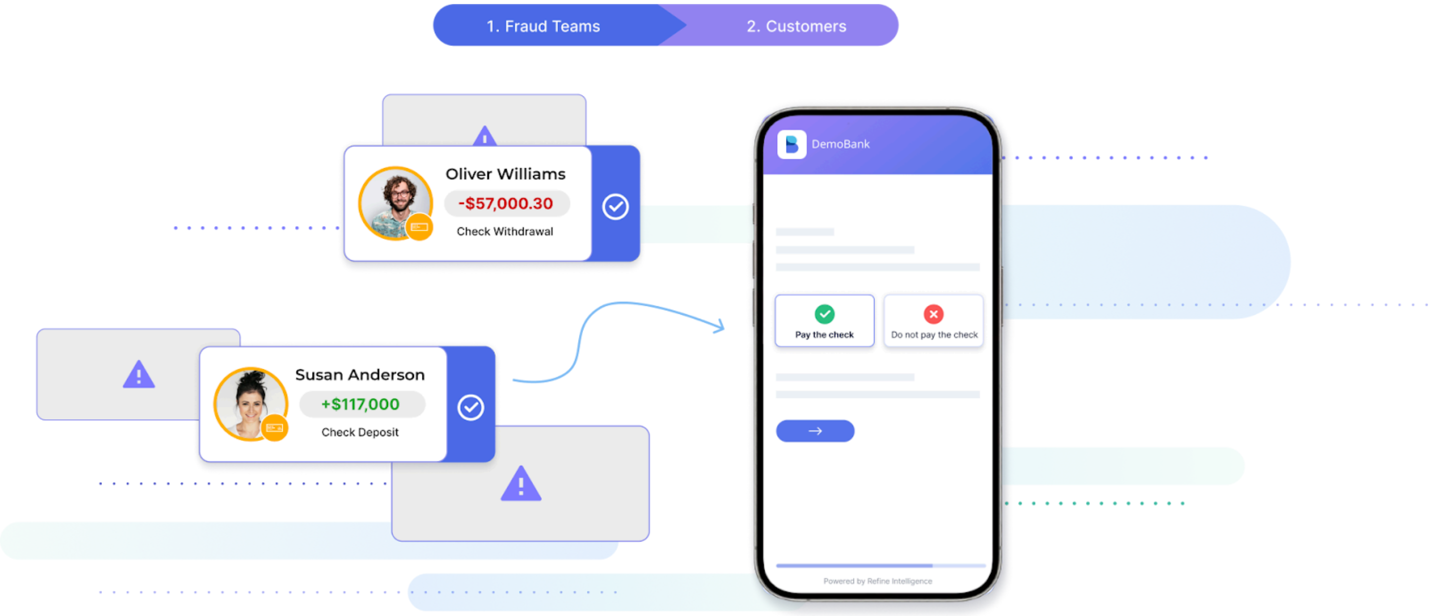
Contextual Data

It is important to gather unique data related to the customer's check history, beneficiaries, payments, associated entities, and digital footprint data (geolocation, device, and network parameters). In order to adopt this approach successfully, banks should follow this best practice:

- **Build a robust check fraud evidence repository:** Support manual investigations alongside direct Virtual RFIs.

Refine's Platform for Check Fraud Prevention

Refine uses Intelligent Customer Outreach and Analytics to resolve saturation in financial crime and compliance. It works with your existing detection system. Banks use Refine's platform to create highly efficient workflows, leverage the 'customer signal' and reduce loss.



Bank customers can resolve their own check fraud alerts. Source: Refine Intelligence

60 seconds

To complete a Digital RFI

Refine's platform sends out automated RFIs that take just 60 seconds to complete, reducing friction while delivering the data that investigators need to make fast, accurate decisions.

Bank investigation teams can create an RFI that will approach the customer using multiple communication channels based on their preferences and bank policy.

Key Benefits

- ✓ Works with any check fraud detection system
- ✓ Tailor the workflow and inquiries to your unique operational needs
- ✓ Scales up prevention through high-velocity RFIs
- ✓ Seamlessly scale your fraud operations with an automated platform
- ✓ Get immediate ROI as you reduce check fraud costs
- ✓ Let your customers validate their checks within minutes

To learn more about how Refine Intelligence fosters direct communications between risk teams, branches, and customers to fight fraud and financial crime, read about our Direct Customer Outreach for Check Fraud solution.

Learn more today. Request a demo.