IN-CLEARING CHECK FRAUD PREVENTION: STOPPING FRAUD AT THE PAYING BANK

An in-clearing check is an item that a paying bank receives from another institution for payment. The check was deposited or cashed by another institution and is now being presented to the paying bank through the interbank clearing system or exchange network. Since this item was not deposited at the same institution the check is drawn on, the paying institution typically has limited visibility into the deposit or check cashing transaction, which could have potential indicators of risk. The siloed nature of this process can make it more difficult to identify certain types of check fraud, such as:

- Counterfeit checks: new checks that look identical to legitimate check stock
- Altered checks: checks where the payee and/or dollar amounts were changed
- Forged checks: checks where the maker's signature is forged
- Forged endorsement: stolen checks that bear forged endorsements

Similar to deposit fraud, countering in-clearing check fraud requires a strong fraud prevention framework built on a layered approach to identify and prevent fraud before losses occur.

LAYERED DETECTION: COMBINING MANUAL ANALYSIS AND TECHNOLOGY

Current-day fraud detection uses a layered approach that combines automation and manual analysis. Although the use of technology is not a new concept for fraud detection, technology uses are evolving. Artificial intelligence (AI) and machine learning (ML) systems have the capability to evaluate millions of data points and flag anomalies in check serial numbers, payees and/or payment amounts. This technology also can analyze images and assess the likelihood of a possible forgery, alteration or counterfeit check.

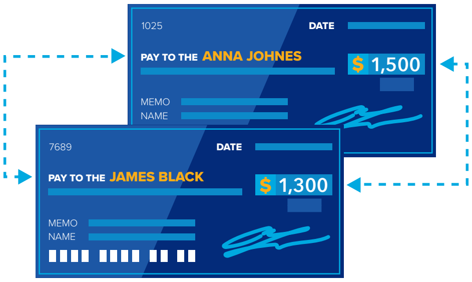
Case study: A financial institution detected a sudden increase in high-dollar checks clearing from an account that was out of pattern for the customer. Within a day, multiple checks over $20,000 were presented for payment by different institutions. The paying bank's fraud detection platform identified the items based on multiple anomalies: the check numbers were out of range, the amounts exceeded the average amount of other checks issued, and there was no history of payments to the payees.

The suspicious in-clearing checks were immediately escalated to a fraud analyst for review —and visual inspection confirmed that the signature on the items was different from the customer's signature. The fraud analyst contacted the customer and verified he had not issued the checks.

IN-CLEARING CHECK FRAUD PREVENTION: STOPPING FRAUD AT THE PAYING BANK

In this case study, the institution was able to return the items and prevent a substantial monetary loss, demonstrating how technology and manual review can work together to protect the institution and the customer against in-clearing check fraud.

Another important tool is a solution that allows the paying bank to validate a check presented for payment by comparing it to a list of checks issued by the customer. The list of checks – typically provided to the financial institution on a daily basis by the customer – includes the issued checks' serial number, amount and often, the payee. This solution enables paying banks to quickly discern which in-clearing checks may be fraudulent and adds another layer of protection, which can help prevent:



- Checks that were stolen and had the maker's signature forged
- Unauthorized remotely created checks
- Check alterations where the amount or payee is changed (if the payee can be validated)
- Counterfeit checks: creating new checks using new payment information or a previously issued check serial number and amount details (if the payee can be validated)

Case study: A commercial customer issued a check for $14,750 to a trusted vendor. The check was stolen, altered and then, deposited using a different payee name.

As the altered check came through the paying institution's in-clearing process, the payee validation system immediately flagged the mismatch between the payee on the check and the payee listed in the customer's file that contained legitimately issued check information. Fraud analysts confirmed the payee alteration and returned the check as altered/fictitious.

This case study exemplifies the benefit of developing a strategy for exception item reviews and efficient escalation workflows. Suspicious items that are escalated promptly to fraud analysts can result in timely, informed decisions, often in collaboration with account holders.

Alternatively, AI/ML and other tools can be used to identify and approve known valid items – reducing the volume of cases sent for manual review by fraud analysts.

Technology solutions can use historical data and context to identify normal behavior and check usage patterns. Technology also can aid in image analysis and signature verification to assess the probability of an image or signature being valid. An organization may consider approving – or passing on – items that have a high probability of being legitimate based on the historical data and image analysis.

IN-CLEARING CHECK FRAUD PREVENTION: STOPPING FRAUD AT THE PAYING BANK

PREVENTION AND FRAUD MITIGATION

Customer education is a key component of prevention. Encouraging customers to use sound practices can help minimize risk of fraud, such as:

- Keeping check stock secure
- Using gel ink
- Filling in checks properly and not leaving blank spaces
- Using available security features on check stock
- Strong internal controls – such as dual authorization where a secondary person reviews and approves the payment
- Promptly reconciling accounts
- Setting up account alerts for quicker notification of certain transactions and contact information changes
- Considering alternative payment methods and avoiding mailing checks

An enterprise-wide fraud management system – where check data is integrated with robust account details and other payment methods and channels, such as ACH transfers, wires, instant payments transfer and card activity – creates a holistic view to prevent fraud. This centralized approach allows institutions to identify the onset of fraud more quickly, detect cross-channel fraud patterns and respond more effectively. Consortium data and fraud intelligence also can be incorporated into fraud management systems and processes – providing institutions with a wider range of signals to detect fraud.

CONCLUSION

Check fraud continues to become more organized and sophisticated. In-clearing fraud – where counterfeit, altered or forged checks are presented for payment through the interbank clearing system – can be a particularly challenging area. Financial institutions can help deter in-clearing fraud by continuously training staff, educating customers on best practices, and enriching fraud models and detection software to adapt to new trends. In addition, leveraging data, technology and manual reviews can help institutions maximize the potential of their available resources.

The check fraud mitigation toolkit was developed by the Federal Reserve to help educate the industry about check fraud and outline potential ways to help detect and mitigate this fraud type. Insights for this toolkit were provided through interviews with industry experts, publicly available research, and team member expertise. This toolkit is not intended to result in any regulatory or reporting requirements, imply any liabilities for fraud loss, or confer any legal status, legal definitions, or legal rights or responsibilities. While use of this toolkit throughout the industry is encouraged, utilization of the toolkit is voluntary at the discretion of each individual entity. Absent written consent, this toolkit may not be used in a manner that suggests the Federal Reserve endorses a third-party product or service.