HOW FINANCIAL INSTITUTIONS CAN RESPOND TO CHECK FRAUD

Effective remediation of check fraud involves rapid containment, clear customer communication, objective investigation, prompt account remediation and continuous improvement informed by post-incident fraud analysis.

1 CONTAINMENT

When check fraud is detected, institutions can benefit from acting quickly to mitigate loss exposure, including:

- **Take steps to protect** impacted account(s) and prevent additional fraud.
- **Review recent and pending account activity** to identify other suspicious transactions.
- **Return or dishonor (decline to pay) fraudulent checks** if within the return window.
- **Promptly file a bank-to-bank or breach of warranty claim**, adhering to time limits based on the type of fraudulent check.
- **Work with law enforcement** for investigation and recovery.

2 FACT FINDING

Work with the customer to confirm fraudulent activity and gather key information:

- **Review transactions** with the customer to identify which checks are fraudulent and identify if there is any other unauthorized activity.
- **Ask questions** to identify if checks have been lost or stolen and determine the type of fraudulent check(s).
- **Obtain an affidavit** from the customer detailing the fraudulent check(s) and type of check fraud that occurred.
- **Inform the customer of next steps** and begin processing the claim.

3 INVESTIGATION

Review the transaction details and information provided by the customer to investigate the fraudulent check(s):

- **Analyze** the check images, transactional data and customer/account history.
- **Document findings and determine** if the customer was negligent (e.g., first party fraud) or if unauthorized party fraud has occurred.
- **Assess next steps** for remediation and recovery (e.g., breach of warranty claims may apply, customer account may need to be reimbursed, etc.).

HOW FINANCIAL INSTITUTIONS CAN RESPOND TO CHECK FRAUD

4 REMEDIATION

Reimburse customer based on findings of the investigation and pursue recovery options:

- **Issue credit to customer(s),** as appropriate, for the fraudulent transaction(s) that cleared their accounts.
- Work with customers to **ensure their accounts are secure**, as applicable, based on any additional findings during the investigation.
- **Initiate recovery attempts** through returns, breach of warranty claims, or indemnification requests.
- **Record and classify** the fraud event and corresponding documentation in an internal tracking system.
- **File reports** for the fraudulent activity based on required thresholds and work with law enforcement if applicable.

5 POST-INCIDENT FRAUD REVIEW

Analyze event details and timeline to identify root cause(s) and provide a feedback loop for ongoing improvement.

- **Identify** if the cause was related to ***people*** (e.g., if a fraudulent check was not identified during an investigative review), ***process*** (e.g., if exception-handling procedures created a vulnerability) or ***technology*** (e.g., a check did not kick out for review).
- Make **informed updates to** prevention and detection rules, strategies or models.
- **Refresh** staff training and customer education to incorporate applicable findings.
- **Escalate** recurring and organized fraud patterns to inform other stakeholders (e.g., branches, contact centers and product teams) about risks.