Allied Solutions

Allied INSIGHTS

Fraud & Security RISK ALERTS

Timely insights to protect against fraud and mitigate risks

Stolen Checks – A Criminal Business

SUMMARY

A recent federal case shows how check fraud has evolved from isolated check washing into an organized criminal supply chain.

According to the U.S. Department of Justice, five defendants used stolen USPS arrow keys to steal mail containing checks and personal information. They then produced counterfeit or forged checks, altered checks to higher amounts and deposited or cashed them using accounts and identification they controlled.

Authorities recovered approximately $1.7 million in stolen checks, six USPS mail keys, 40 debit and credit cards in other individuals' names and extensive personal information. Two defendants also moderated a Telegram group of approximately **2,000 individuals through which stolen checks were sold.**

THE RISK

Financial institutions should not view check fraud solely as a forged-instrument problem. Organized groups can obtain genuine checks, account information and signatures directly from stolen mail, then use that information to create convincing counterfeit or altered items.

A fraudulent check may therefore contain authentic account and routing information, familiar formatting and a genuine or convincingly reproduced signature. Visual inspection alone may not identify the fraud.

The check may look legitimate. The deposit activity may not be.

RECOMMENDED MITIGATION STEPS

1. Strengthen Check Deposit Controls

- Monitor newly opened accounts for unusually high check deposit volume or dollar amounts shortly after opening.
- Apply appropriate holds and enhanced review to suspicious or unusually large checks, consistent with institutional policy and applicable law.
- When specific facts create a well-grounded belief that a deposited check is uncollectible, consider using the Regulation CC reasonable-cause exception. Document the factual basis, provide the required notice, retain applicable records and ensure the hold period is reasonable. The exception should not be applied solely because of the check type or class of depositor.
- Review checks for alterations to the payee, amount, date, signature, MICR line and check number.
- Pay particular attention to items that appear washed, chemically altered, photocopied or digitally reproduced.
- Use available check-fraud detection, duplicate-detection and verification tools.

2. Monitor for Account Takeover and Mule Activity

- Identify accounts receiving multiple checks drawn on unrelated individuals or businesses.
- Monitor the rapid movement of deposited proceeds through ACH transfers, wires, ATM withdrawals, P2P payments or cash withdrawals.
- Establish monitoring for newly opened accounts exhibiting immediate high-volume or high-dollar check activity.
- Review recent changes to contact information, login credentials, devices or authentication settings that precede unusual deposits or outbound transfers.
- Escalate accounts displaying characteristics consistent with money-mule activity.

3. Enhance Frontline Detection

- The customer is not the registered owner.
- The account is new or recently opened.

- Multiple or unusually large-value bonds are presented.

4. Protect Against Mail-Related Check Fraud

- Encourage business account holders and high-volume check issuers to use **Positive Pay or Payee Positive Pay** where appropriate.
- Recommend secure mailing practices, including depositing outgoing mail inside a Post Office or secure collection point and promptly retrieving incoming mail.
- Promote electronic payments when practical for recurring or high-dollar transactions.
- Encourage account holders to use transaction alerts, reconcile check activity frequently and report missing checks immediately rather than waiting for a monthly statement.

5. Review Check Numbers and Account Activity

- Monitor for out-of-sequence or duplicate check numbers.
- Identify checks clearing significantly outside established dollar, payee or transaction patterns.
- Monitor deposits made through channels or locations inconsistent with the account's normal activity.
- Review sudden changes in check amounts, payees or transaction frequency.
- When available, compare suspicious items with images of previously paid checks to identify differences in check stock, formatting, MICR information or signatures.

6. Establish a Rapid-Response Process

When a suspected stolen, counterfeit or altered check is identified:

- Preserve the front and back of the check image, endorsements, supporting documentation and available deposit-channel metadata.
- Contact the account holder promptly through a verified communication channel.
- Determine whether additional checks or account information may have been compromised.
- Review recent and pending transactions for related activity and place appropriate alerts or restrictions consistent with policy.
- Contact other affected financial institutions promptly through established bank-to-bank channels to pursue return or recovery options when appropriate.
- Direct potential victims of mail theft to the U.S. Postal Inspection Service or 1-877-876-2455.
- Report suspected criminal activity to the appropriate law-enforcement agencies and follow applicable SAR and other regulatory reporting requirements.

- Evaluate time-sensitive return, warranty and indemnity options with counsel. Depending on the facts, these may include UCC transfer or presentment warranties and applicable Regulation CC provisions governing electronic checks or substitute checks.

KEY FRAUD PREVENTION MESSAGE

The Miami Gardens case demonstrates that stolen checks can become commodities within an organized criminal network.

Financial institutions should evaluate more than whether a check looks legitimate. Effective detection considers the entire transaction: the instrument, depositor, account history, deposit channel, source of the check, movement of funds and consistency with the account holder's normal behavior.

RISK MITIGATION RESOURCES

- Financial Crimes Enforcement Network – Financial Trend Analysis
- USPS – Mail Theft FAQ
- Visit our Fraud Prevention Center to learn best practices on protecting against U.S. Savings Bond Fraud

Need assistance or want to request a consultation?
Contact our risk specialists at risk_specialist@alliedsolutions.net

The information presented in this email is intended for informational purposes only and should not be construed as legal advice or a legal opinion and it may not reflect the most current legal developments. You should seek the advice of legal counsel of your choice before acting on any information provided in this email.