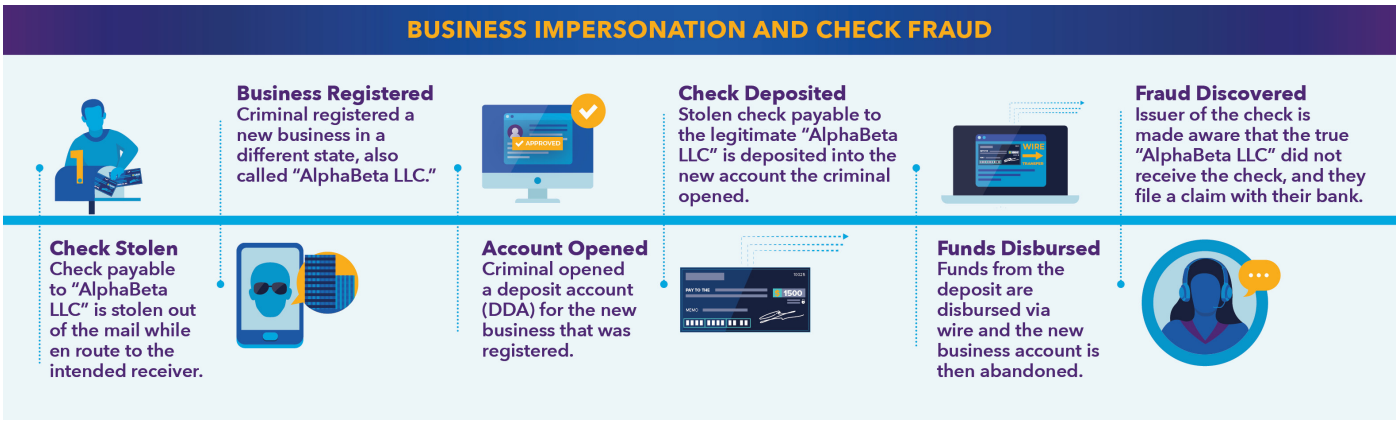
HOW CRIMINALS COMMIT CHECK FRAUD USING STOLEN BUSINESS IDENTITIES

The growing rate of checks being stolen from the mail has been highlighted by the Federal Bureau of Investigation (FBI), U.S. Postal Inspection Service, Financial Crimes Enforcement Network (FinCEN) and payments industry surveys. Once stolen, checks most frequently are altered or counterfeited. Given these trends, financial institutions are focusing on prevention strategies to make attempts to negotiate fraudulent checks – especially ones for large amounts – less lucrative for criminals. However, since a large percentage of businesses continue to mail checks to pay other businesses, criminals remain incentivized to exploit vulnerabilities and use new tactics to thwart those prevention strategies.

One tactic is to impersonate the payee on the stolen check – leaving the check in its original condition to attempt to bypass alteration and counterfeit check detection tools. ***If the stolen check is payable to a business, the criminal may register a new business with the same name as the intended payee but in a different state, instead of changing the payee on the check.***

THE TREND: NEW BUSINESS, DIFFERENT STATE



This trend does not require the criminal to alter or counterfeit the stolen check before depositing it. Instead, it leads to a fraudulent endorsement that could take the issuer of the check months to identify – giving the criminal plenty of time to access the funds and disappear.

Variations of this trend also may help criminals to successfully impersonate a business and elude detection when depositing a stolen check, including:

- Creation of a synthetic business registration that intentionally uses a very similar name as the payee/business on the stolen check.
- A criminal who assumes the identity of the business by changing, or pretending to be, an authorized party on the business registration or with the financial institution.
- Opening a DBA (Doing Business As) account to mimic the legitimate payee/business.

HOW CRIMINALS COMMIT CHECK FRAUD USING STOLEN BUSINESS IDENTITIES

THE IMPACT

Financial institutions, businesses and consumers may incur financial losses from fraudulently endorsed checks that were deposited and cashed. The issuer of the check may not immediately realize it was stolen and not received by the intended payee, creating a window of opportunity for the criminal to access the funds and disappear.

WHAT CAN FINANCIAL INSTITUTIONS DO?

While greater awareness of business identity theft and its connection to check fraud is an important first step in mitigation, the layered nature of this type of fraud makes it more difficult to detect. Criminals are methodical and organized, often ensuring the business documentation to open the fraudulent new account is consistent with legitimate businesses. The checks, while stolen, were legitimately issued and can bypass some payment verification controls.

Combating this type of fraud involves targeted strategies throughout business account opening processes and check deposit channels, as well as a coordinated analysis across both of those activities. There typically is not a single indicator of fraud. However, financial institutions might consider additional investigation if anomalies are identified in business identification, the individual opening the account and/or when checks are deposited shortly after account opening. A robust Know Your Customer (KYC) program and holistic evaluation of the new account, including the potential risk of the individual opening the account, can help mitigate this risk. The assessment can be done in person, at the branch or through a digital account opening process – and should consider how criminals attempt to socially engineer employees and seek vulnerabilities within digital processes.

Although this is not an inclusive list, the following indicators may warrant additional investigation:

Business

- Consortium data indicates discrepancies leading to potential identity fraud, such as "true name fraud" where the legitimate business information is used by someone not authorized to conduct activity on behalf of that business
- Business geographic location provided is different than the incorporated entity's
- Information collected through the new account application process is inconsistent with data available through external sources – such as data aggregators and consumer reporting agencies
- Articles of incorporation, bank statements and other business documentation are unavailable, appear to be falsified or contain inconsistent information

HOW CRIMINALS COMMIT CHECK FRAUD USING STOLEN BUSINESS IDENTITIES

Individual

- Identity information of the "authorized owner" of the business opening the account raises concerns during the KYC process
- The individual opening the business account does not appear to have a clear understanding of what type of business it is or what they do
- Identification indicates implausible geographic distance between individual's location and the business

Check Anomalies

- Date of the deposited check is before the date the business was registered
- Payee/business on the check is in a different state than the address on file for the deposit account that was opened
- Inconsistent locations for the business address, authorized signer identification or the location of the sender/receiver according to the check

Financial institutions also may find it helpful to educate their commercial customers about business identity fraud. While there is no silver bullet to prevent business identity theft, businesses can monitor their registration status, authorized signers, account activity and business profiles. In addition, checks have been a common form of payment for most businesses – primarily for small businesses. The preferred usage of checks – and the fact that most businesses state they mail checks to pay other businesses – highlight an opportunity for financial institutions to educate their commercial customers about alternative payment methods, especially when payments are issued for large amounts.

CONCLUSION

Business identity theft and check fraud can be a highly lucrative combination for criminals. The way in which criminals structure their fraud schemes requires a thoughtful, dynamic strategy to combat them. Enhancing awareness and identifying attributes within each step criminals take to commit check fraud can help detect the next fraud scheme in an earlier stage. A constant cycle of refinement is essential to help safeguard against the evolving tactics used to commit check fraud.

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.