FAKE COMPANIES, REAL RISK: THE RISE IN SYNTHETIC BUSINESS FRAUD

Synthetic business fraud is an evolving risk that involves fabricating a business identity to commit fraud. This can be done using real or fictitious information, such as a real tax ID number combined with a fake business name and address. Once created, criminals use these synthetic businesses to deceive financial institutions by opening accounts to access credit, loans and other banking products. Typically, businesses have access to higher credit or loan amounts than consumers, making them more attractive to criminals. This can result in larger losses when a default on repayment occurs.

Traditional fraud controls and detection methods may not consistently identify these fake companies. However, financial institutions can leverage lessons learned from combating synthetic identity fraud to help safeguard their portfolios against synthetic business fraud.

CREATING A NEW SYNTHETIC BUSINESS

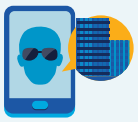
Stolen, manipulated or manufactured information is used to create a fraudulent corporate entity, such as an address, telephone number and business officer's name. Criminals then register the "business" with an agency in the state where the firm will "operate," often the secretary of state's office. Operators typically can register their businesses online for accessibility and convenience. However, lack of in-person verification may make it easier for criminals to submit fabricated information. In addition, a business entity can apply online or use other methods to request an Employer Identification Number (EIN) from the Internal Revenue Service (IRS). To support the credibility of a new synthetic business, criminals may create a company website and use social media to display contact information and fake customer reviews.

CRIMINAL USES FOR SYNTHETIC BUSINESSES

- **Lines of credit:** Criminals apply for a line of credit at a financial institution based on fabricated business information. If approved, they may quickly withdraw the maximum available amount or overdraw the line with no intent to repay.
- **Other loans:** Criminals may falsify financial statements and overstate their collateral when applying for a loan from a financial institution. When a loan amount is approved, criminals then can withdraw or move the full amount and not repay the loan.
- **Money laundering:** Criminals can attempt to disguise the proceeds, sources or nature of their illicit activities by opening business accounts to receive and move money.
- **Invoice fraud:** Criminals can use a synthetic business to submit fake invoices to legitimate companies for goods or services that were never provided.

FAKE COMPANIES, REAL RISK: THE RISE IN SYNTHETIC BUSINESS FRAUD

SYNTHETIC BUSINESS FRAUD EXAMPLE



1

A criminal creates a synthetic business, "America LLC," to fraudulently obtain a business loan.

2 REGISTER

The business registers with the secretary of state's office and applies online for an Employer Identification Number (EIN) from the IRS.

3

The criminal creates a company website with a contact phone number, email address and service descriptions.

4

He opens a business account with a financial institution and makes transactions to add legitimacy and build credit history.

5

The criminal then applies for a $250,000 business loan, allegedly to invest in marketing and increase sales.

6

A synthetic identity is used as the loan guarantor on the application supported by false financial statements and tax returns.

7

The financial institution does not identify any red flags in its due diligence.

8

The loan is approved and funds are quickly withdrawn, then immediately moved to money mules (people who help criminals transfer illicit funds) and cryptocurrency wallets.

9

Loan payments are not made. The financial institution subsequently cannot contact the business.

10

The financial institution's investigation reveals that the business owner and loan guarantor are both synthetic identities.

11

The financial institution takes a loss for the full loan amount.

FAKE COMPANIES, REAL RISK: THE RISE IN SYNTHETIC BUSINESS FRAUD

FACTORS FUELING SYNTHETIC BUSINESS FRAUD

Synthetic business fraud is growing based on several contributing factors.

- Registering a new business with a state agency is intended to be easy for owners. Criminals can submit online forms without appearing in person for verification.
- The business registration process is an administrative function designed to provide new business tax IDs. It is not intended to detect false company information or synthetic businesses.
- Financial institutions may expect standard Know Your Customer/Know Your Business (KYC/KYB) requirements to detect synthetic businesses. However, KYC/KYB requirements may not be able to detect that a company was created using false information.
- Criminals use sophisticated technologies to make synthetic businesses appear to be legitimate. For example, generative artificial intelligence (AI) can be used to produce fake identification and business documents to facilitate opening company accounts. In addition, it can be used to create company logos, descriptions of products and services, websites and social media profiles to add credibility to a synthetic business.

PREVENTING AND DETECTING SYNTHETIC BUSINESS FRAUD

Financial institutions may seek to prevent and detect synthetic business fraud with a multi-layered approach, which often focuses on identifying potential risks based on a review of company information, account activity and company behavior. Examples of potential red flags:

Inconsistent business information

- Business details don't match public records, including state business registration records
- The physical address does not exist or is not consistent with a business (e.g., it is for a house, apartment building or empty lot)
- There is no business website or social media profile, or the content appears generic
- The business owners and officers have a limited credit history and sparse public records (e.g., phone numbers and physical addresses)
- Business information (e.g., a phone number) matches that of other corporate entities or accounts, which may indicate these details were re-used

FAKE COMPANIES, REAL RISK: THE RISE IN SYNTHETIC BUSINESS FRAUD

Suspicious account activity

- Larger-than-typical dollar amounts and volume of transactions for a new business
- Transactions are not consistent with the expected business type
- The geographic location of the company's IP address (a numeric designation that identifies its location on the internet) is not near the business address

Unusual business behavior

- High revenue claimed for a newly registered business
- Immediate and aggressive requests for access to credit lines or loans
- Inconsistent business activity explanations
- Frequent updates to the business profile and contacts

Since criminals often attempt to open accounts with multiple financial institutions using the same or similar information, sharing intelligence about potential synthetic businesses with other organizations can assist detection. For example, using details provided by another financial institution may help detect a synthetic business via matching data, such as its tax ID number, email address or phone number.

CONCLUSION

Synthetic business fraud is an increasing threat to financial institutions, with the potential to result in even more significant losses. This type of fraud can be difficult to detect due to the sophistication of tools used by criminals to appear credible and the lack of comprehensive sources to validate companies. However, financial institutions' tactics to mitigate synthetic identity fraud for consumer accounts also can help identify synthetic businesses. These tactics include increased collaboration and information sharing, strengthening account opening controls and applying proven synthetic identity fraud detection strategies.

The synthetic identity fraud mitigation toolkit was developed by the Federal Reserve to help educate the industry about synthetic identity 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