Understanding B2B Fraud

Types of B2B Fraud

You Can’t Fight What You Don’t Understand

Instances of business-to-business fraud have increased dramatically, with fraudsters exploiting a variety of circumstances triggered by the global pandemic. B2B fraud has the potential to cripple businesses with millions of dollars in losses. But knowledge is power; this white paper will increase awareness of evolving fraud schemes and discuss the newest tools and methods for detecting and preventing fraud.

In the wake of COVID-19, instances of commercial fraud became much more likely as businesses, financial systems, and service providers of all types were put under extreme pressure to respond and adapt to the crisis.

A recent report from the Association of Certified Fraud Examiners found that 51% of organizations responding to the survey have uncovered more fraud since the onset of the pandemic. Fully 71% of survey respondents expect the level of fraud impacting their organizations to increase over the next year.

Why Has Fraud Been Increasing?

What accounts for the exacerbated vulnerability of businesses to instances of fraud? One major factor: during the pandemic, many businesses shifted their operations to become “digital storefronts” rather than physical locations. They had to, because of the dramatic change in customer buying behavior, with transactions largely taking place online due to fears of virus transmission.

The other major factor was the shift to remote work, which increased a variety of risks related to the vulnerability of data, devices, and files. Many employees were working on unsecured networks and personal computers that could be more easily penetrated by fraudsters. Reduced oversight and decentralization of tasks—such as generating payments—also made instances of fraud harder to detect.

In light of expectations for fraud to continue to proliferate, all businesses and capital market participants need to have a plan to battle online fraud on a continuous basis. But before you can make a plan to combat something, you need to be sure that you understand it. What do we mean when we refer to “fraud”? What types of fraud are specific to businesses, rather than individuals? And what are the red flags that organizations need to learn to recognize?

Types of Commercial Digital Fraud

There are, unfortunately, almost as many types of fraud as there are colors in the rainbow. Here is a selection of the most widely occurring frauds.

EMPTY SHELLS

One of the most common types of frauds is the creation of shell, or shelf, companies that are created for the sole purpose of committing fraud. These companies allow fraudsters and criminals to hide identities and motives, conceal the origin, flow, and destination of funds, and obscure the true beneficiaries of fraudulent activity.

“Empty shell” fraud schemes include:

- Limited to no business activity relative to business nature and time in business
- Using synthetic identity to create a new business or reactivate an inactive business

MISREPRESENTATION

Another burgeoning fraud type is business misrepresentation—defined as material malfeasance and deception through the fabrication, exaggeration, or omission of business data. This type of fraud cuts across both first-party and third-party fraud observed in the marketplace.

Misrepresentation fraud schemes can include:

- Exaggeration of employee headcount, time in business, or annual revenue
- Alteration or fabrication of bank statements or utility bills

NEVER INTENDED TO PAY

In many online transactions, the fraudster opens a new business account and purchases goods or services and then doesn't make a single payment. These fraud schemes can sometimes be detected during onboarding with the analytic indicator of probability of first payment default.

Characteristics of these fraud schemes include:

- Opening accounts with real or synthetic identity, but no intention of paying on them
- Boosting credit limits artificially and through manipulation of data

"BUSTING AT THE SEAMS" FRAUD

In the "Commercial Bust-Out" scheme, the fraudster opens many lines of credit and eventually abandons all accounts after maxing out or exceeding all credit lines. Using available firmographic, digital identity, and prior fraud incident data along with analytic indicators can help identify such actors.

These fraud schemes can involve:

- Making on-time payments and maintaining good account standing for months or years before committing fraud
- Making overpayments with bad checks in the final stage of "bust-out"

STOLEN IDENTITIES

We're familiar with identity theft when it comes to individuals. A similar approach is used by fraudsters when it comes to business identity theft. This is where the perpetrator acts as the business owner or representative of a legitimate company. Using the "borrowed" credentials of a legitimate business, a fraudster can engage with another business in ways that ultimately reduce cash flow, cause problems with creditors and suppliers, and even affect the business's reputation.

These schemes can include:

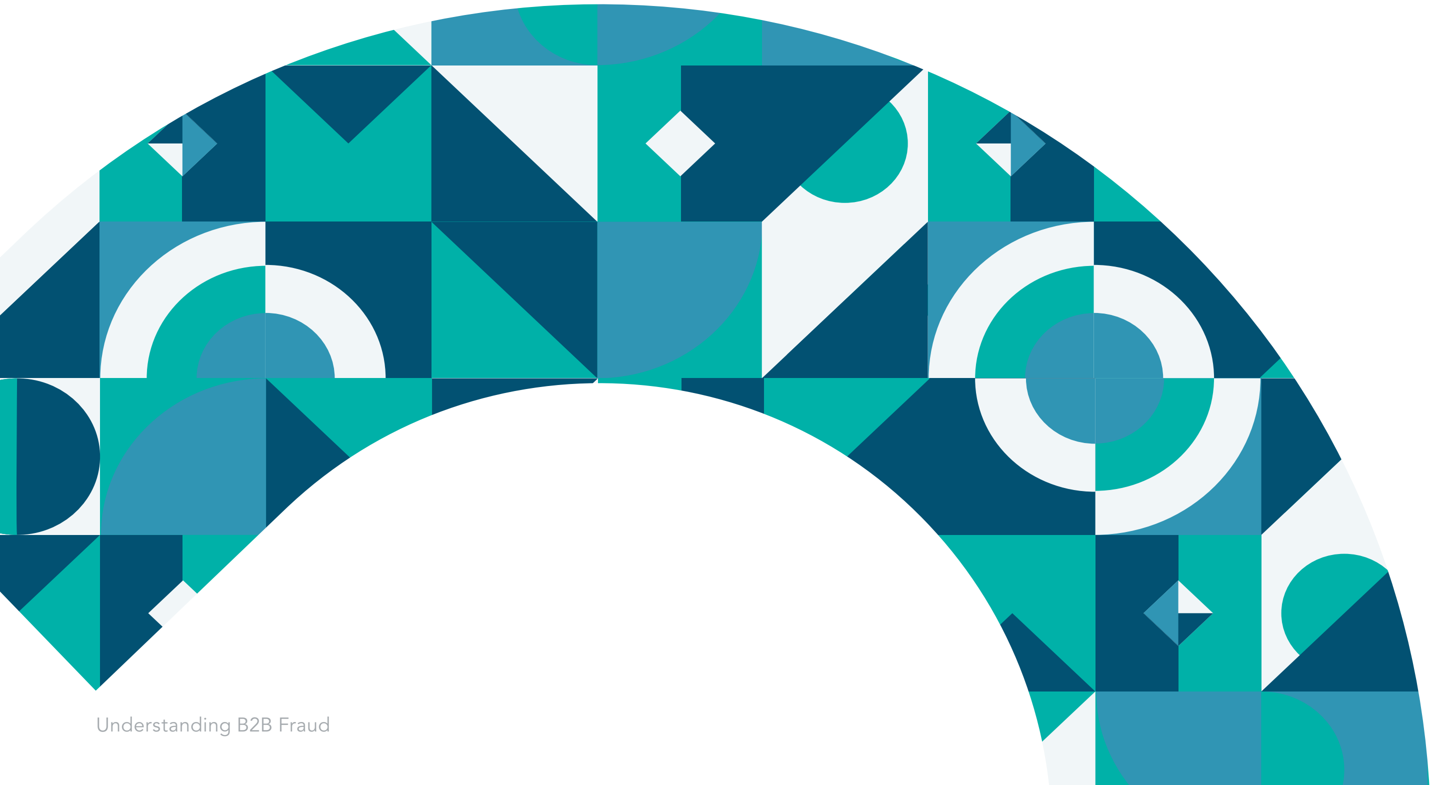
- Establishing temporary office space or merchant accounts in another company's name
- Filing bogus documents with government or credit agencies to change another business's registered address or the names of the directors and officers
- Using a business email domain not linked to the company domain for transactions

"MOVE OVER, I'M TAKING OVER"

Another example of observed fraud is "account takeover," where the fraudster compromises an existing account of a legitimate business. In this dangerous development, the perpetrator can redirect accounts payable to a different account, siphoning off significant funds before being discovered.

Types of "account takeover" schemes include:

- Phishing and malware attacks
- Harvesting data from data breaches or dark web purchases



What You Need to Know to Protect Your Business

Now, let's look at how companies can reinforce their defenses against fraud by implementing a multi-layer fraud risk assessment framework.

A fraud risk assessment framework is a process that helps pinpoint areas where an organization may be vulnerable to fraud so it can develop concrete fraud mitigation plans. Conducted correctly, a fraud risk assessment framework keeps the business a few steps ahead of fraud perpetrators by viewing the company holistically from a fraudster's perspective. The framework guides the effort to answer questions such as: where do we have weaknesses in our controls that could be exploited? And in what ways could our organization inadvertently be helping fraudsters escape detection?

To be effective, a fraud risk assessment framework has to have several foundational, data-driven layers. The first layer comprises the effort to accurately identify potential customers or third parties—who they actually are, and whether they present possible risks or discrepancies based on company data. The second layer involves scrutiny of the digital identity markers associated with those entities—electronic credentials that will help establish a comprehensive business fraud risk profile during real-time transactional processes. The third layer involves evaluating operational and financial factors.

FIRST LAYER

Verifying Identity—Is This a Legitimate Business?

The point when a business or supplier initiates a new business relationship is the best time to conduct the necessary due diligence to verify a company's legitimacy. This process relies on data—optimally, data that has been rigorously vetted using multiple sources to ensure the business genuinely and uniquely exists.

Lower-risk profiles are characterized by greater consistency between self-reported business data and reference data. Inconsistencies within this data often signal a higher-risk profile and a higher likelihood of attempted fraud. These inconsistencies include minor discrepancies that might be dismissed as accidental errors but are actually deliberate. For instance, a fraudster may add an "S" or "Inc." after a legal business name to create a "look-alike" company name.

Fraudsters will fabricate, exaggerate, or even omit certain data elements to make their business look more established. For example, a business may claim it started operations in 2015. But reliable data sources show that this business was created in 2021. By claiming 2015 as the business incorporation year, the fraudster could then exaggerate the annual employee count, sales revenue, or operational volume so the overall business profile appears to be more credible—thus creating opportunities for the entity to conduct fraud.

Investigating an entity's address is an important identity verification step. Typically, higher risk is associated with virtual office locations, P.O. boxes, residential addresses, and freight forwarding addresses for a business transaction.

Key questions to ask during this phase of fraud risk assessment include:

01 What is the firmographic information for the business, and can it be verified?

02 Businesses don't commit fraud, individuals do—so can we identify the individuals behind the business?

03 Is the business identity legitimate or synthetic?

04 Were the principals involved in any previous, now-defunct businesses?

05 What products are they purchasing, and does it make sense for this business to do so?

SECOND LAYER

Uncovering Risks Behind a Device, IP, or Email Address

When the global pandemic brought the physical world to a grinding halt, fraudsters took advantage of the moment. Dun & Bradstreet data shows a 251% increase in business identity theft in 2020, compared with 2019 (Figure 1). This spike is strongly correlated with dramatic increases in digital transaction volumes and related cyberattacks. More consumer identity data getting into the hands of bad actors translates to more occurrences of B2B fraud.

Typically, fraud rings use a handful of IP addresses or hosts and cycle through a long list of stolen user credentials to breach a company's security/fraud defenses. For this reason, assessing fraud risk based on the email, domain, phone number, or device and IP address being used for transactions is critical.

In particular, email age is a telling risk indicator. For example, an email address established two days before it was used in a commercial loan transaction would be highly irregular. Data analysis has shown a higher incidence of fraud activity connected to newer emails.

For instance, if a real business domain is abcpizza.com, a fraudster might create abcpizzainc@pizzaparlor.com, instead of first.last@abcpizza.com. In one real-world example, a fraudster placed a large order for restaurant equipment, and instead of using the real business domain abcpizza.net, the fraudster used the "look-alike" of abcpizza.us.

When researching a domain as part of a fraud risk assessment, a best practice is to look at the "whois" information. It will be important to understand when the domain was created and compare that against the company start date.

The device profile will need to be captured real time to evaluate device risk. Key considerations include device age, velocity, reputation, and device IP.

- Device age will detect a device new to the network.
- Device reputation is highly effective in identifying devices previously used for fraud.
- Velocity will gauge If the same device is being used to create multiple accounts within a short period of time.
- Device IP can detect geolocation mismatches between the business's operating location and the device location.

One benefit of using device risk data is that the device ID provides anonymous computer characteristics, rather than personal information, to help create a digital profile for fraud detection. If a business account has already been rejected due to suspicious behavior, and the fraudster uses the same device to apply for another account under a different name, the organization will know right away because the returning device can be verified.

A comprehensive fraud risk assessment framework is much broader than what has been described here; organizations also need to examine their existing fraud control processes, map them to different fraud schemes, and implement appropriate activities to remediate fraud control gaps. But having quality data that can authenticate an entity's physical and digital identities, and thus prevents fraudsters from gaining access to the business, saves valuable time and intercepts many major fraud schemes before they can cause financial and reputational damage.

Annual Increase in Business Identity Theft Cases

2016–2020

Source: Dun & Bradstreet

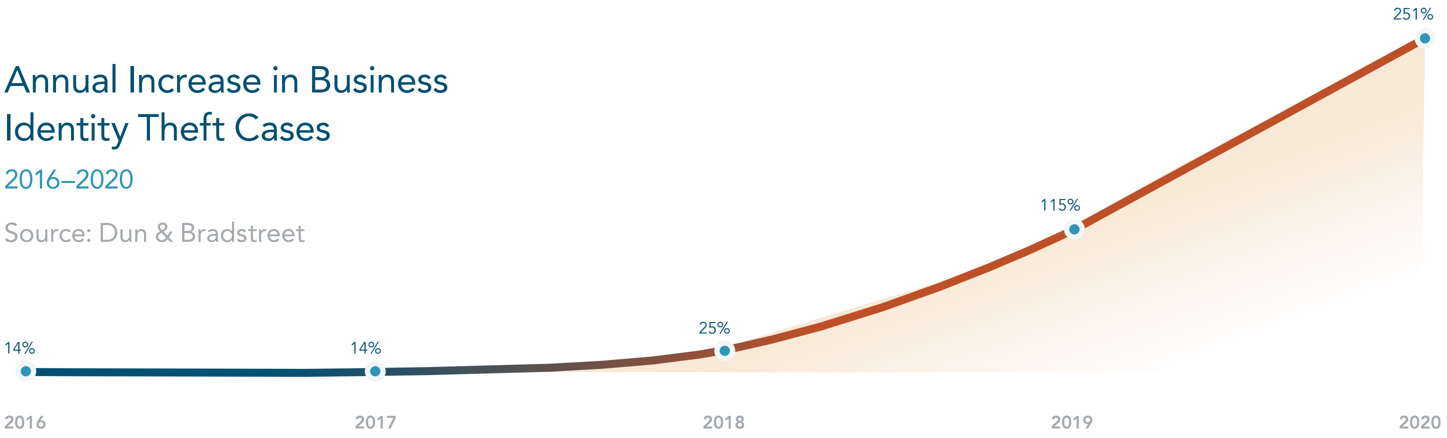


FIGURE 1

THIRD LAYER

Evaluating Operational and Financial Factors

Although it can be challenging to differentiate first-party fraud risk from more typical credit risk, both during the application process and after onboarding, the key distinction is intent—active use of deception to obtain goods and services for financial benefit with no intent to pay. When evaluating fraud risk, the financial incentives for the potential first-party fraudster are important considerations.

As an example, a company may be consistently making payments on time and is considered a low credit risk. But then the company starts maxing out its credit line and eventually defaults on all its payments. This is typical "bust-out" behavior. It demonstrates a fraudster's level of skill and patience in gaming the system. When activity like this comes to light, it should trigger an examination of the financial health of the business or vendor you are dealing with and closer scrutiny of its transactional behaviors over time.

Key questions to ask during the fraud assessment process include:

- Is the business making more credit inquiries than usual? Has it started spending to the limit of its credit line?
- Is the business making timely payments?
- Is the company trending up or down on key financial metrics?
- Is it already delinquent or on the brink of bankruptcy?

Operating status, activity level, and time in business are part of the equation. Consider **Company B** in the table that had been inactive for a while, and only recently resumed operating with major changes in business name, address, phone, and ownership. There might be a legitimate ownership transfer—or, on the other hand, this might be a case of business identity theft by a fraudster without the real owner's knowledge.

Establishing a brand-new business requires a significant amount of effort. In contrast, leveraging an existing business shell to commit fraud is much simpler. In the table, the highlighted aspects of **Company B**'s profile would indicate that this company presents a higher fraud risk than **Company A**.

COMPANY PROFILE COMPARISON*

Company Aspects	Company A	Company B
Time in Business	10 Years	
Operating Status	Inactive several years; recently resumed operations	
Business Registration Recently Restated	No	**Yes**
Ownership and/ or Contact Details Changed	No	**Yes**
Transactional Data Depth	Rich	**Thin**
Recent Inquiry Increase	No	**Yes**
Financial Risk Assessment**	Low risk	

*Data supplied by third-party data provider; this is essential for a comprehensive fraud risk assessment. **Based on bankruptcies, delinquencies, or other red flags regarding the company's viability. Because company B was inactive until recently, no evidence of this type appears in its profile.

Combating Fraud

The Good News

To fight fraud effectively, companies need to achieve a higher level of awareness of fraud and its various types. Thanks to increased press coverage of pandemic-related fraud schemes, this greater awareness is starting to take hold. Greater awareness will produce more internal conversations around fraud and fraud risks. Anti-fraud professionals will have an opportunity to capitalize on these conversations to argue for more resources to bolster their fraud detection and prevention programs to keep pace with the changing nature and volume of business fraud schemes.

D&B® Fraud Risk Insights helps finance teams better identify precursors and safeguard their organization against potential fraudsters by adding a layer of intelligence to auto-decisioning without slowing down the approval process.

This suite of analytics helps to enhance due diligence processes and protect a company's bottom line from losses associated with first- and third-party fraud, specifically business representation, business identity theft, and 1st payment default.

For more information, contact your Account Executive.

ABOUT DUN & BRADSTREET®

The information provided in articles are suggestions only and based on best practices. Dun & Bradstreet is not liable for the outcome or results of specific programs or tactics. Please contact an attorney or tax professional if you are in need of legal or tax advice.

dnb.com