dun & bradstreet

EBOOK

Transform from Reactive to Ready: Building Smarter B2B Fraud Risk Strategies

Experts liken digital business-to-business (B2B) fraud to the flu virus: Both are widespread, constantly evolving, and more dangerous than many people realise. That can make them hard to detect — and hard to get rid of.

Though technology can be used to help protect businesses from B2B fraud, cybercriminals and bad actors are also using it to perpetrate thefts, breaches, and other malfeasance.

For instance, generative artificial intelligence is helping bad actors create convincing false identities and social engineering for targeted, highly personalised attacks. With AI-created deepfakes, fraudsters can use audio and video to impersonate business leaders and scam victims into surrendering sensitive information and cash. As real-time payments and cryptocurrencies have grown, so has the volume of push payment scams, business email compromise (BEC), investment schemes, and other malicious attacks.

Contents

Where Do Fraudsters Get Their Information?

In addition to AI and other technologies, bad actors are increasingly using data and services from the open, deep, and dark web. This powerful combination is enabling them to commit digital B2B fraud on a much broader scale — and more quickly — than ever before.

The open web, also called the surface web, is the portion of the internet that is publicly accessible and includes websites, blogs, and social media. Generally intended for positive purposes, this content (particularly social media) is also leveraged by cybercriminals to prey upon unsuspecting businesses.

The deep web — private databases, email accounts, online banking, and other information that requires authentication or is not available to the general public — is where fraudsters are gaining information to help them breach security controls, infiltrate business networks, and collect sensitive data on product plans, litigation, financial results, and more.

The dark web, a subset of the deep web, is intentionally hidden and requires specific software to access. It is often associated with illegal activities, but it also hosts forums and websites for privacy-focused users. It's there that fraudsters are buying personal identity data as well as information on companies' security vulnerabilities and controls.

The popularity of open-source software (OSS) — estimated by researchers to be used in more than **90%** of all applications — has also captured the attention of cybercriminals.

Because open-source software and code are publicly accessible, fraudsters can potentially exploit reported vulnerabilities before patches and other defenses are launched. They may also appropriate and misuse open-source tools intended for legitimate security testing. Generally easy to install, OSS may be slipped into businesses that lack stringent IT and security policies, inadvertently creating blind spots and open doors where bad actors can obtain all kinds of information.

Here's where our analogy is helpful again. The keys to avoiding, diagnosing, or recovering from the flu – just like B2B fraud – are education and healthy habits. So the first step to fighting digital B2B fraud is to learn what the most common forms are and understand why they're growing.

What Are Common Types of B2B Fraud?

B2B fraud tends to fall into one of two categories: first-party fraud or third-party fraud. First-party fraud is perpetrated directly by an individual or a specific business to defraud or steal from you. Third-party fraud is usually committed by a third-party actor who appears to be another person or company in order to access and steal your business's goods or services.

First-Party Fraud Examples

COMMERCIAL BUST-OUT

A business remains current on account payments for some time before making overpayments with bad checks, eventually maxing out all credit lines and abandoning all accounts.

SHELL OR SHELF COMPANIES

These are fictitious or legitimate entities that engage in little or no business activity. They are used to hide identities and motives, conceal the flow of funds, and obscure true beneficiaries.

BUSINESS MISREPRESENTATION

This type of fraud cuts across both first-party and third-party fraud. It is material malfeasance and misrepresentation based on the fabrication, exaggeration, or omission of business data.

FIRST PAYMENT DEFAULT

In this scheme, fraudsters open a new account for a real or synthetic entity and then never make a single payment on any debt owed.

Third-Party Fraud Examples

BUSINESS IDENTITY THEFT

A perpetrator acts as the representative of a legitimate company, and using the "borrowed" credentials, engages with other businesses in ways that cause financial, supply chain, and reputation issues.

ACCOUNT TAKEOVER

In this scheme, a fraudster compromises an existing account of a legitimate business to redirect accounts payable to a different account in order to siphon off funds.

SYNTHETIC IDENTITIES

A bad actor blends real identifying information from a business and/or its officers with other fictitious information to create a new business entity or impersonate an existing business.

BUSINESS EMAIL COMPROMISE (BEC)

Cybercriminals impersonate a trusted colleague or peer and trick a company employee into sending money, revealing sensitive information, or performing other risky acts.

Why Is Digital B2B Fraud on the Rise?

Historically, when economies experience volatility or contraction, the risk of fraud tends to increase. As consumers spend less, businesses reduce inventories, and suppliers receive fewer orders. With less cash in circulation, cybercriminals become even more vigilant for weaknesses they can effectively exploit for theft and financial gain.

Consider, for instance, the growth of digital transactions. Real-time payments and cross-border commerce in particular have expanded the opportunities for B2B fraud.

The speed of payment and lack of reversibility make real-time payment systems attractive targets for cybercriminals. In addition, engaging customers across multiple continents means that businesses must accommodate different languages, currencies, regulations, and technologies — and the resulting complexities can help perpetrators more easily disguise themselves and their efforts.

For similar reasons, global operations and diversified supply chains can create significant challenges for vendor management and account verification. This expansion can strain a business's security systems, monitoring and analysis capabilities, and vendor management resources — all of which can enable bad actors to operate more quickly and covertly.

Geopolitical instability, trade wars, sudden regulatory changes, and higher interest rates are helping to complicate lending and financing, adding to companies' financial pressures. With so much attention focused on maintaining cash flow, fraudsters are finding more creative and sophisticated digital methods to access credit, avoid collections, and escape detection.

Cybercriminals often run their schemes using a common playbook. They invest time and money to create their own entity (or establish a false one) to perpetrate fraud and theft within a particular channel until they're discovered. In an organised and systematic fashion, they simply move to another channel and "rinse and repeat" with the same misleading business, avoiding the expense of building a new entity for as long as possible.

Three Key Questions to Help Assess Risk Exposure

Understanding what form digital B2B fraud is likely to take, and the conditions that can help it thrive, is an important step for protecting the business that you've built. The next step is to conduct a fraud risk assessment.

By focusing on **three key questions**, you can identify processes or functions where your business may be weak. Then use those insights to help your organisation develop an effective fraud mitigation and prevention strategy to correct and strengthen them.

01 Which of your potential B2B customers, vendors, or suppliers are legitimate businesses?

The best time to conduct due diligence to verify a company's legitimacy is the point at which you decide you want to initiate a business relationship with that company.

Due diligence relies on data — optimally, third-party data that has been rigorously vetted. Lower-risk profiles are characterised by greater consistency between self-reported business data and third-party reference data. Inconsistencies can signal a higher-risk profile and a higher likelihood of attempted or potential fraud. Keep in mind that fraudsters may also fabricate, exaggerate, or omit certain information to help make their fake business seem well-established and upstanding.

Researching an entity's address is important. Typically, higher risk is associated with virtual office locations, P.O. boxes, residential addresses, and freight forwarding addresses for a business transaction. Don't forget to review any prior and/or defunct businesses in which the owners or principals were involved.

It's critical that businesses also establish and communicate clear internal policies for ongoing monitoring, updating, and sharing this data. At a minimum, your policy should indicate the frequency of formal re-evaluations of portfolio data and should document how anomalies or exceptional events will be assessed. These policies help ensure that your customer and supplier data remains reliable, trustworthy, and valuable so you can more easily spot potentially harmful entities.

02 What are digital identity markers revealing about prospective customers, suppliers, or vendors?

Typically, fraud rings use a handful of IP addresses or hosts, and then 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, 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.

When researching a domain as part of a fraud risk assessment, a best practice is to look at the WHOIS public database. It is important to understand when the domain was created and compare that date against the company's start date.

Device profiles and IP addresses are valuable for creating a digital profile to support fraud detection. The device profile should be captured in real time to effectively evaluate device risk. Be sure to examine:

- **Device age:** Helps you identify a device that's new to a network
- **Device reputation:** Highly effective in identifying devices previously used for fraud
- **Velocity:** Helps gauge if the same device is being used to create multiple accounts within a short period of time
- **Device IP:** Helps spot geolocation mismatches between the business's operating location and the device location

A benefit of using device data is that the device ID provides anonymous characteristics, rather than personal information. So if a business account was rejected due to suspicious behavior, and the fraudster uses the same device to apply for another account under a different name, the fraudster can be discovered more rapidly because of the repeated use of that original device.

03 What financial and operational behaviors do potential customers and providers exhibit?

Scrutiny of a business's financial and operational behavior can yield important insights into possible intentions to deceive and commit fraud. Watch for red flags, starting with whether a vendor or customer is making more credit inquiries than usual, or if it has started spending to the limit of its credit line.

Check to see if that business is making timely payments and whether it is trending up or down on key financial metrics. Find out if the business is already delinquent on payments or appears to be on the brink of bankruptcy.

Be sure to review business registrations; bad actors have taken particular interest in secretaries of state and the opportunities to compromise business registrations. In some states, it's cheaper to compromise and reinstate a business than it is to form a new business. Carefully examine the filings that have occurred on that subject business and check for any anomalies, changes, or reinstatements.

Don’t Let Your Guard Down

Unfortunately, avoiding digital B2B fraud isn’t a “one and done” activity. Fraudsters, once discovered, are unlikely to go away. Like a virus, they tend to morph in order to maximse their impact on their intended targets.

Minimising or preventing attacks requires current, comprehensive, trustworthy data to help you recognise the signals and develop an effective defense for your business. Beyond better data and analytical insights, experts point to crucial habits that can help you fortify your risk position.

- First, be proactive, and consistently monitor and communicate with your customers, vendors, and suppliers.
- Check your own business credit reports vigilantly, just as you would your personal consumer credit reports, for accuracy and integrity.
- Examine your existing fraud control processes, map them to different B2B fraud schemes, and implement appropriate activities to remediate fraud control gaps.
- Work closely with your tech and data analytics teams to collaborate on data intelligence that can help your business identify anomalies and risky behaviors for internal and external contacts.
- Join networks and consortiums to help share your findings with peers so that patterns and methods can be widely studied and mitigated.
- Finally, don’t forget to make employee education and training a priority; knowledgeable employees can be your strongest line of defense against digital B2B fraud when they understand how to effectively fend off determined cybercriminals.

ABOUT DUN & BRADSTREET®

Dun & Bradstreet, a leading global provider of B2B data, insights and AI-driven platforms, helps organisations around the world grow and thrive. Dun & Bradstreet's Data Cloud fuels solutions and delivers insights that empower customers to grow revenue, increase margins, manage risk, and help stay compliant—even in changing times. Since 1841, companies of every size have relied on Dun & Bradstreet.

dnb.com