dun & bradstreet

Busting Bust-Out Fraud

Five steps for combatting bust-out business fraud

In an *Annual Report to Nations*, occupational fraud accounted for some 5 percent of a typical company's annual revenue.[1]

THE RISE OF BUST-OUT BUSINESS FRAUD

A number of factors are fueling the growth of bust-out frauds. The Internet makes it much easier today for fraudulent companies to register for state and local business licenses, establish virtual offices in prominent office buildings, create shell companies, and obtain other proofs of right as legitimate businesses. Disreputable credit coaches and so-called business enhancement services provide guidance to fraudsters on how to set up a fake business and obtain credit without arousing suspicion. At the same time, competitive pressures make many companies reluctant to turn away new customers; and sales personnel, eager for a sale, may even coach new customers on how to skirt their own company's anti-fraud controls. Bust-out fraudsters usually disappear with the stolen money or goods long before the victimized companies realize they've been cheated and payment is never coming.

Business fraud does not receive the high-level of attention given to consumer fraud. In many instances, companies do not even know they have been the victims of fraud, which they often mischaracterize as bad debt and then take it off their books. In addition, many companies are reluctant to even acknowledge losses due to fraud, preferring to quietly absorb their losses as a cost of doing business. Consequently, the exact cost of business-to-business fraud is not known. However, studies by Dun & Bradstreet suggest that the financial losses due to fraud can range from one-half percent to five percent of a company's annual sales, depending on the industry and company. That's a high cost of doing business, especially when cost-effective strategies exist for significantly reducing fraud risk without slowing legitimate sales.

AN ENVIRONMENT RIPE FOR FRAUD

From the criminal's point of view, "bust-out" business fraud is an ideal scam. You can target multiple companies—both large and small—in a single operation; your fraudulent activities fly under the radar of most traditional anti-fraud controls; and you can abscond with the stolen cash or goods before your victims even realize they've been scammed. In a case still under investigation by law enforcement officials, a phony California business acquired a state business license, leased warehouse space, built an e-commerce website, created a false corporate history, and established other Proofs of Right that persuaded at least 50 companies to extend credit to this seemingly legitimate business operation. The companies included medium and large businesses, including Fortune 500 companies, that leased equipment and sold office suppliers, computers and electronics, and other consumable goods that are easily re-sold. Once the credit agreements were in place, the fraudulent business quickly borrowed against its limits and then disappeared without paying for the goods it obtained from its unsuspecting creditors. All together, the victimized businesses were exposed to over $2.8 million in losses.

This scenario is being replayed throughout the United States and abroad. In today's digital age, fraudsters have little trouble creating the trappings of what appears to be a legitimate business. They often operate from a virtual office address, use the Internet and online services to establish a virtual phone number, answering service, government business registration i.e., LLC and licenses, favorable, yet fake financial statements, made-up trade or payment references, and even steal the identity of another business with favorable credit history. They carefully research each targeted company to understand, for example, how the company verifies creditworthiness and how much credit they can request without triggering a more rigorous background check. This new generation of criminals has essentially blown up the traditional model for verifying a new business customer's Proof of Right and legitimacy.

[1]Association of Certified Fraud Examiners (ACFE), *Report To Nations On Occupational Fraud and Abuse*.

BUST-OUT BUSINESS FRAUD DEFINED

Scam, hoax, misrepresentation, deception, cheat, sting, swindle, con. These are all terms that apply to fraud. The perpetrators of business fraud typically obtain cash and/or goods through normal business transactions but with one important twist: They never intend to pay. Essentially, business fraud is stealing carried out through carefully planned misrepresentation and deception.

Bust-out fraud is a common and growing type of business fraud. In a bust-out fraud scenario, the perpetrators create a seemingly legitimate company by using traditional "proofs of right." Once established, the fake company applies for credit from multiple vendors, enticing them with the expectation of a mutually profitable business relationship. The fraudsters then draw upon the maximum amount of credit approved by each vendor.

In a "straight-roller" bust-out fraud, the perpetrators make no attempt to pay. As their invoices go past due for 30 days, 60 days, 90 days, and so on, they may offer promises of payment or excuses while they complete their scam, but they never pay. In more complex bust-out frauds, the perpetrators may pay some or all of the initial invoices in order to negotiate for an even higher credit limit. They will then "max out" their new, more lucrative credit ceiling and then disappear without paying.

Companies recognize that they are increasingly vulnerable to this costly fraud threat, but they are uncertain how to implement cost-effective controls that can reduce fraud risk without slowing sales or driving away legitimate customers.

NEW APPROACHES FOR COMBATING FRAUD

New technologies and methodologies are needed to give companies the advantage in the fight against business-to-business fraud. No single solution will solve the problem, but by taking a series of layered actions, companies can not only significantly reduce the risk of bust-out fraud, but they also can provide decision makers with greater transparency into their business partners and customers, and into other risks to the company's bottom line. The new avenues for combating business fraud are:

– **Beyond Basic Business Information.** Companies collect vast amounts of data about business customers, partners, and suppliers; and today, many new sources of business information are available to enhance insight. These new sources include: sales and CRM entries, shipment data, labor market data, sentiment (or opinion) data, government data, merchant data, utility data, social media, and other non-traditional data. After discovering the data available from third party sources – as well as from across the organization internally – the next step is to curate the data to derive insights and drive systematic decisions based upon these insights. This process needs to be constantly evaluated and improved, thereby making it virtuous and beneficial at reducing business fraud.

– **Anticipatory Analytics.** With the help of powerful and factual analytics programs, companies can analyze their combined or united data-sets to gain insight into their business customers and partners. Buried within the mounds of data are "red flag" patterns or indicators of potential fraud. Anticipatory analytics sift through the noise to uncover fraud signals—that is the likelihood that fraud may occur—to help companies identify risks and target appropriate actions to minimize those risks. Analytics can provide a warning of potential payment delinquency, never paying and first payment default, or ceasing operations by customers.

– **Innovative Technologies.** Companies can take advantage of new technologies and services that cast a light on fraudsters hiding in the shadows. For example, device fingerprinting technologies can collect information from remote computing devices, even when the cookies are turned off, to identify the devices that are being used in transactions with the company. This enables companies to identify individual devices by their activities, such as the accounts they access, so companies can stop doing business with devices that are involved in suspicious activities or previously were used to perpetrate fraud with other companies who have deployed these technologies.

– **Employee Education and Expectation.** Your employees, particularly your sales staff, are the first line of defense against fraud. Understandably, many are reluctant to adopt stricter measures that might drive away legitimate customers. They want to make it easy—not difficult—to do business with your companies. Consequently, it's important that your employees understand their role in the company's overall fraud mitigation strategy. They should be first notified of their role and then trained to ask the right questions, recognize risk indicators that warrant further investigation, apply new anti-fraud tools, and report suspect fraud to a centralized unit. Their participation and support in developing procedures for vetting customers without slowing the sales process will significantly reduce fraud risk. Providing timely feedback on tips reported or learned about is critical to deputizing them and providing updates on the latest patterns and trends that the fraud unit observes. By extending the fraud responsibility beyond the credit and fraud department to the entire organization is a best demonstrated practice.

– **Public-Private Partnerships.** State and local governments want to prevent criminals from obtaining government-issued business licenses, registrations, or permits to facilitate their fraudulent activities. Like the businesses they are trying to protect, government agencies also want to implement safeguards without slowing or discouraging legitimate businesses within their jurisdictions. Given their joint interest in combating fraud, the public and private sectors should work more closely together to identify emerging trends and best practices among corporate and government agencies, including statutes to prosecute offenders. The public sector should embrace the collaboration and responsibility to identify tools and techniques that reduce business fraud without placing a burden on legitimate businesses to register for business licenses, registrations, certifications and the like.

D&B STRENGTHENS BUSINESS-TO-BUSINESS FRAUD PREVENTION

The enemy in any conflict has an equal say in the methods and approach they deploy. Criminals are constantly adapting their tactics, seeking new ways to mask their activities, so they can strike and then disappear before their victims catch on to their scams. Government and business must be equally adaptive. Dun & Bradstreet, which provides in-depth coverage of more than 235 million businesses in over 1,000 industries across the globe, is strengthening our business data, analytic capabilities, and insights to help our customers proactively confront fraud head-on. We are:

– **New Sources of Data—New Ways to Combat Fraud.** Vast amounts of new data are available that can provide insight into companies and their executives, such as social media, labor market data (e.g., job postings), government data, and utility data, all of which can be mined for information and insight. Our systems are proficient across multiple languages and writing systems—D&B is the only provider of multi-lingual Identity Resolution—so we can gather and integrate global business information. And are continuously improving data quality and governance. With our expanded data collection capabilities, we now collect verified, multi-sourced intelligence from more than 30,000 sources worldwide.

– **Anticipatory Analytics Not Only Predicts, But Prevents Fraud.** Identifying and preventing fraud requires the ability to distill and then transform into insight the subtle signals from multitudes of data. To develop a suite of anti-fraud solutions, we analyzed 50,000 business variables from many sources to identify those that are the most predictive of fraud and other types of business risk. These solutions incorporate advanced analytics to analyze numerous risk factors, such as a company's payment history, spend behavior, financial obligations, size, commercial activity, as well as trends and velocity of these same signals. Our suite of solutions leverage new proprietary and customer data sources to identify extreme-risk companies to customize and predict bust-out fraud, first-time payment default, business identity theft, account takeovers, and other type of acute risk.

In combating business fraud, D&B faces many of the same challenges as our customers. Fraudsters try to manipulate D&B databases in order to create false business identities and misrepresent themselves as legitimate companies, and so we employ many of these same anti-fraud techniques and analytic solutions to identify suspicious companies and prevent them from perpetrating fraud—against us or our customers. We draw upon this experience as we partner with companies to help them refine their policies, implement best practices, train staff, and tailor solutions to strengthen their overall fraud-prevention posture. D&B leverages a fraud consortium that brings together representatives from government and industry to discuss ways that stakeholders can work together to combat business fraud. During annual fraud forums, members exchange lessons learned and identify emerging trends and best practices among corporations and government agencies. They also identify available tools and techniques that reduce the risk of business fraud without placing a burden on legitimate businesses at the point of sale.

CONCLUSION

There is no silver bullet for eliminating bust-outs and other types of business fraud, but companies can stay ahead of fraudsters' changing tactics and schemes with a multi-layered approach that leverages new sources of information, anticipatory analytics, emerging technologies, robust employee training, and collaboration with other public- and private-sector stakeholders. Such efforts generate a positive return on investment that goes beyond fraud prevention, because they also strengthen a company's overall management of its customers, partners, and suppliers, as well as increase visibility and improve decision-making across the organization. Most importantly, companies can implement proactive strategies that mitigate fraud risks while facilitating fluid customer transactions to power the successful business enterprise.

UPDATE

The people behind the California bust-out scheme described on page one are still at large. The total losses likely exceed $4Million. Additionally, we are actively working a number of other cases that have the same methods and likely the same individuals.