WHITE PAPER

Enabling Commerce. Mitigating Business Fraud.

August 2013

Strategies for businesses to stop fraud without slowing commerce

Business fraud is growing at an alarming rate. Many companies struggle to counter the increasingly sophisticated tactics of criminals who use phony business identity credentials to obtain credit and then disappear. Businesses can retake the advantage in the fight against fraud with a proactive strategy that applies the major principles of managing risk to combating business fraud.

Executive Summary

Business fraud is growing at an alarming rate. Many companies struggle to counter the increasingly sophisticated tactics of criminals who use phony business identity credentials and partial truths to obtain credit and then disappear with stolen money or goods before their deception is discovered. Businesses can retake the advantage in the fight against fraud with a proactive strategy that applies the major principles of managing risk to combating business fraud:

- Swift and decisive alerts of potential fraud at the point of sale, followed by continuous monitoring throughout the customer lifecycle.
- Strong verification and authentication capabilities linked to real-time access to robust and reliable sources of business data.
- Benchmarking and the constant tracking of fraud to continuously improve fraud prevention processes.
- Closed loop information sharing among businesses and government entities to strengthen fraud prevention capabilities, both individually and collectively.

By following these four principles, businesses can significantly mitigate the risk of business fraud without disrupting legitimate sales, and put in place an infrastructure that is ever alert to changing fraud tactics and threats.

Commercial Fraud: Where the Money Is

When asked why he robbed banks, legendary bank robber Willie Sutton allegedly replied, "Because that's where the money is." Today, white collar criminals are targeting commercial businesses for various types of fraud, knowing that many companies are increasingly vulnerable to digital-age scams. Consider these statistics:

- The estimated cost of commercial fraud in the United States now stands at more than $11 billion annually.[1]
- Business identify theft has surpassed $4 billion annually and is now one of the most popular forms of commercial fraud, growing 13 percent annually.[2]
- The typical business credit fraud is 10 times larger than consumer credit fraud.[3]
- External and internal fraud costs companies an average of 2.1 percent in annual earnings.[4]

New Technologies, New Fraud Tactics

Business fraud is not new, but criminals today are using new technologies to devise elaborate schemes that are difficult to detect until long after they have disappeared with the stolen money or goods. For example, criminals are using online registration systems and databases to falsify information in order to strengthen their credit reports and fraudulently obtain credit. Criminals can also give their companies a false appearance of stability and prosperity by renting professional receptionists and virtual office space that comes with a prime business address. Similarly, they may purchase shell or shelf companies that provide a business history and appearance of legitimacy. Conversely, instead of establishing phony companies, many criminals are simply stealing the identities of existing businesses by co-locating at the address of a legitimate business or going online to falsify business registration records. This enables them to use the good name and credit of the legitimate company to secure credit and purchase goods for fraudulent gain. After establishing credit through identity theft or other means, the criminal company uses its credit, often legitimately at first, and then increases its purchases and vanishes without paying. These "Bust-

1 D&B Customer Research, 2011
2 Javelin Study, Identity Fraud Survey Report, 2010
3 Business Week, July 2007
4 Kroll Study, 2011

Out" frauds create huge unpaid debts for the businesses and banks that extended credit.

"We have seen an increase in fraud in the commercial space and a trend in the types of fraud committed becoming more sophisticated," said Kathleen Wachholz, Severe Risk, Dun & Bradstreet (D&B). "Fraudsters have gotten smarter in their approach, recognizing they need to be able to pass undetected through today's first generation fraud tools. In addition, on some occasions, we have seen fraudsters combine consumer identity theft with the creation of a fraudulent, fictitious business to get past existing detection tools."

Inadequate Tracking of Fraud

Why is business fraud growing? Many businesses lack the processes and capabilities to detect these increasingly sophisticated frauds. The Internet has made it easier for fraudsters to steal identities, fake traditional "proofs of right" demonstrating legitimacy, attack multiple industries, collaborate and share information with other criminals, and operate anywhere in the world. Moreover, as law enforcement, banks, and businesses crack down on individual identity fraud, many criminals are shifting to business identity theft, where the safeguards are not yet as strong and the payoff is much more lucrative. Because the many types of business fraud are difficult to detect, they often go unreported as fraud and are simply counted by companies in the broader category of bad debt. In fact, many companies do not track fraud carefully, and so may not always know when they have been victims of fraud; and neither do they share information extensively with law enforcement or industry peers. The lack of rigorous tracking and coordination among industry and law enforcement organizations emboldens criminals and makes it easier for them to continue perpetrating scams.

WHAT IS FRAUD?

Criminals are inventing as many ways to commit fraud as there are terms to describe it.

Definition: deceit, trickery, sharp practice, or breach of confidence, perpetrated for profit or to gain some unfair or dishonest advantage.

Synonyms: misrepresentation, duplicity, fraudulence, sham, swindle

Fraud Thrives on Fear of Lost Sales

A major reason why many businesses do not take stronger action is that steps to mitigate fraud are often seen as "friction" in the sales process that drives away legitimate customers. Balancing the need to prevent fraud against the need for a smooth buying experience is not unlike the challenge faced by cybersecurity professionals, who must protect networks without disrupting the information flow necessary for smooth and efficient operations. If network security is too restrictive or slows network traffic, users may try to circumvent security processes, thereby undermining security and making their organizations even more vulnerable to attack.

Similarly, overly strict or cumbersome fraud-prevention controls could drive away legitimate customers, who will go to companies whose fraud mitigation steps are less onerous. Sales staff, worried about losing commissions, may ignore fraud-prevention procedures they consider too restrictive; even worse, they may coach customers on how to circumvent the mitigating steps. The fear of lost sales is particularly strong during economic downturns, making businesses loath to enforce strong anti-fraud measures. Many businesses have come to believe that the cost of fraud, though high, is not as high as the cost of friction in the sales process. For these businesses, fraud is simply an unfortunate but unavoidable cost of doing business.

Four Principles for Proactively Fighting Commercial Fraud

A robust anti-fraud program will span three broad, interrelated areas: Fraud Prevention; Detection and Inspection; and Recovery and Learning (see Figure 1). The challenge facing today's businesses is how to implement needed capabilities and controls in each of these areas without disrupting sales processes or jeopardizing legitimate sales. While fraud strategies will vary based on the size and type of business and volume of sales, companies can easily get started tackling business fraud at their corporation with an at-a-glance checklist based on lessons learned (*see Appendix A for at-a-glance checklist*).

In fact, public and private-sector institutions that deal with credit risk have long faced a similar challenge: How to determine quickly whether an applicant poses

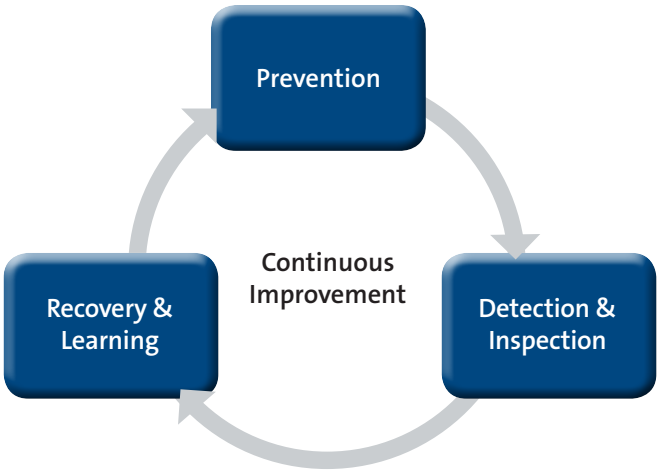

Figure 1: Combating Business Fraud

an unacceptable risk to default on credit? Lenders, whether banks or businesses, don't want to turn down opportunities to extend credit to reliable customers, but neither do they want to extend credit to people who likely will default. And so they have developed ways to quickly measure the level of risk posed by applicants and decide whether to extend credit (and on what terms). Although the factors or variables for measuring credit risk are different from those for calculating fraud risk, the basic principles for mitigating credit risk apply to the various types of commercial fraud. Consequently, four overarching principles should guide companies as they implement fraud-mitigation solutions:

- **Swift and decisive alerts** of potential fraud at the point of sale, followed by continuous monitoring of accounts throughout the customer lifecycle.
- **Strong verification and authentication** capabilities linked to real-time access to robust and reliable sources of business data.
- **Benchmarking and the constant tracking** of fraud to continuously improve fraud prevention processes.
- **Closed loop information sharing** among businesses and government entities to strengthen fraud prevention capabilities, both individually and collectively.

Companies will adopt solutions to fit their organizational culture and processes as well as their specific industry. For example, research shows that telecommunications companies are typically focused on preventing frauds perpetrated through identity theft, fictitious businesses, and never paid/first payment defaults. In contrast, financial services companies are generally more concerned with preventing cross-channel fraud, including check fraud and debit card fraud. By following these four principles, companies from all industries will be able to implement solutions that effectively mitigate fraud risk and provide a measureable return on investment (ROI).

Swift and decisive alerts of potential fraud at the point of sale, followed by continuous monitoring of accounts throughout the customer lifecycle. The

process for identifying fraud at the point of customer contact or sales—red flags, triggers, or other indicators of potential fraud—must be swift and decisive as well as reliable. This requires organizations to implement strong verification and authentication processes and tools at the front end of orders and transactions. The five Cs approach to fraud prevention developed for government agencies can provide companies with a strategic framework to guide their efforts to incorporate verification and authentication activities within existing organizational processes and information technology systems (*see 5Cs box*). Companies also must adopt clear policies for applying their fraud-prevention rules and processes. Equally important, all levels of staff must be educated and trained to follow good fraud-prevention practices. Effective fraud identification and mitigation requires an all-hands-on-deck approach to arm employees with the knowledge, tools, and confidence they need to combat fraud.

Strong verification and authentication capabilities linked to real-time access to robust and reliable sources of business data. Companies that process a high volume of new customer applications must be able to confidently authenticate the business and/or individual associated with the business. Consequently, the fraud mitigation model—the automated methodology and tools that support decision-making–must have real-time access to authoritative business data to provide the required verification and authentication. In today's global economy, this means the model will rely on a global database of business information that is independently and continuously updated with the latest information. The model will incorporate rules and policies for the automated review of portfolios for patterns, velocity, and outliers that may require further inspection. The ideal solution should authenticate the business and/or individual using multiple business and individual authentication data sources; and algorithms can be devised to provide either a simple "pass-fail" response or allow for a more sophisticated decision tree to assess and approve transactions. The model also will provide e-mail or phone notifications of customer changes (*see Figure 2 for an example of a risk-based fraud mitigation model*).

THE FIVE Cs OF FRAUD PREVENTION

Confirmation: Does the person or entity truly exist?

Condition: Is the business and/or its executives active?

Consistency: Are stated facts consistent with other sources of information?

Character: Are there any past issues that could impose risks on the current or a future transaction?

Continuity: Has the current operational status changed and is it posing new risks?

The fraud mitigation model should be robust enough to stand on its own as an off-the-shelf capability that can be acquired and implemented by all businesses, whether large or small; and it also should be flexible enough so it can adapted to a company's internal processes and, if required, customized to prevent frauds specific to the company's industry.

Benchmarking and constant tracking of fraud to continuously improve fraud prevention processes. Businesses must benchmark and track fraud in order to measure progress, develop lessons learned, and provide feedback to strengthen their fraud-prevention activities. For example, as a first step, a business should evaluate its entire customer portfolio and benchmark its "true" fraud loss exposure, including the types and portion of first-payment defaults that are fraud. In addition, the business should develop an executive dashboard for easy tracking and reporting; the dashboard can track fraud by region, date, office or sales location, channel, product type, type of fraud, and other characteristics.

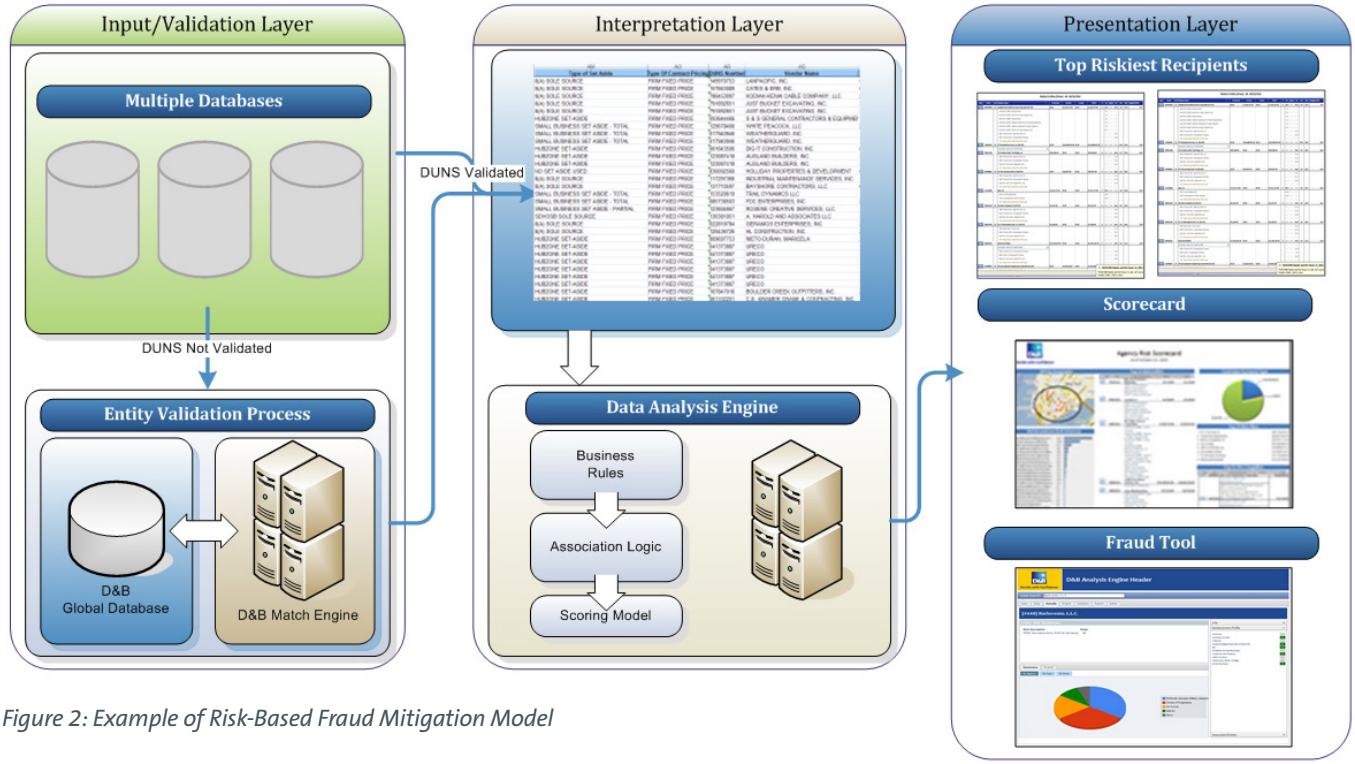

Figure 2: Example of Risk-Based Fraud Mitigation Model

The information gained through tracking can be used in a variety of ways to strengthen fraud prevention. A business can develop its own "Hot Data Files" of bad company names, hot addresses, suspect principal names, suspect registered agent names, heavy loss zip codes or counties, and first-time payment defaults. A business can also communicate its successes to deter future fraudulent attempts. The information gathered through tracking will give insight into the criminals targeting the company and their tactics, as well as into the company's vulnerabilities; and these insights will generate lessons learned to help leaders improve processes, training, and tools, including the fraud mitigation model.

Closed loop information sharing among businesses and government entities to strengthen fraud prevention capabilities, both individually and collectively. Fraudsters rely on secrecy and shun publicity, preferring that their activities remain in the shadows. This ensures that targeted businesses will not be alert to the warning signs of fraud. Businesses can help bring criminals out from the shadows by sharing with each other the information they gather about the frauds and attempted frauds perpetrated against their businesses.

The information might include the tactics, company names, executive names, and other information about the fraudulent businesses. Companies should also build relationships and share cases with the appropriate government entities, such as the U.S. Secret Service, FBI, state and local police, Secretaries of State, and business registration agencies. They also should vigorously investigate fraud and actively work with law enforcement to prosecute cases.

Currently, businesses do not typically share information, preferring to address fraud on their own. But if businesses collaborate and share information with industry peers by creating a closed-loop clearinghouse of fraudulent activity and patterns, they can help each other avoid scams and assist law enforcement in taking criminals off the street and recovering lost property and money (*see Figure 3 for how a fraud data repository works*).

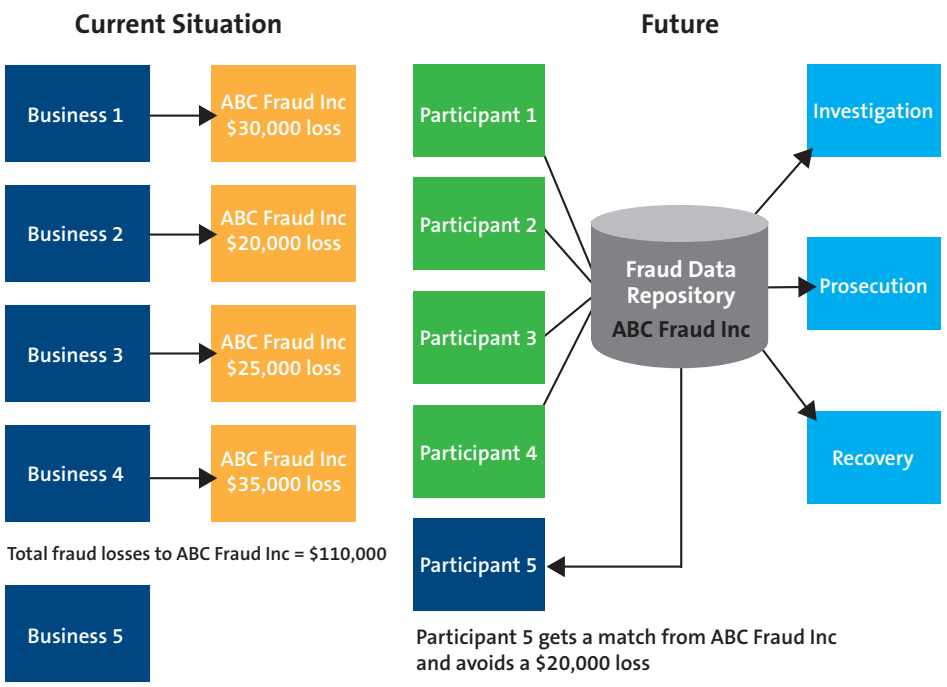

Figure 3: How a Fraud Data Repository Can Prevent Fraud

Conclusion

Businesses are being targeted for fraud because many criminals find it easy—too easy—to deceive businesses to obtain credit for the sole purpose of stealing money and property. Fraudsters cleverly use new information technologies to enable their crimes; and they constantly change their tactics, looking for new ways to scam people. When one door is shut, they look for another.

Businesses can seize the advantage against even the most sophisticated fraud tactics by adopting the four principles of proactive fraud prevention. By applying these principles, business can keep pace with fraudsters' changing tactics by continuously tracking and monitoring fraud, and then updating their databases, processes, and employee training with new information gathered from tracking. In addition, by collaborating and sharing information with both government and industry organizations, businesses can gain additional insights and data to inform their fraud-prevention efforts. With this approach, fraud prevention becomes an organic part of business operations and sales processes, not something that is "bolted on" and so slows and disrupts sales. All employees are trained and engaged in the company's fraud-prevention program. As a result, businesses can be confident and proactive in identifying potential fraudsters and mitigating fraud risks, while still maintaining smooth customer transactions that enable the business to thrive. ■

D&B FRAUD FORUM—AT WORK, PREVENTING FRAUD

As government and commercial entities recognize and respond to the growing threat posed by business fraud, D&B has created a fraud consortium that brings together representatives from federal, state, and local governments and industry to discuss ways that stakeholders can work together to combat business fraud. During the annual fraud forums, members exchange lessons learned and identify emerging trends and best practices among corporations and government agencies as well as identify available tools and techniques that reduce the risk of business fraud without placing a burden on legitimate businesses during a point of sale.

Members also contribute to a commercial fraud risk repository that stores shared fraud information from participating companies. Participants contribute their high-risk data to D&B on a regular basis, while D&B will process the data and make it available only to the participants. In addition, D&B provides participants with ongoing statistics from the database, such as the number of participants and records. This repository can serve as a national reporting database of high risk events, allowing for rigorous analysis and reporting of trends as they evolve, thus enabling participating companies to respond quickly and take proactive action to prevent fraud.

Members also have visibility to new fraud prevention solutions as they become available—such as authentication and verification tools, enhanced high-risk alerts and alert flags, and enhanced fraud scores and analytics—all which enable real-time evaluation and on-the-spot decisions at the point of sale.

This collaboration among businesses and government combats fraud without slowing revenue streams.

Appendix A—Business Fraud Prevention—Getting Started Checklist

Business Fraud Prevention – Getting Started Checklist	
Prevention	Make fraud prevention a high priority—use examples to make your case Implement strict policies and processes to detect business fraud, web fraud and credit card fraud Verify information in the order/application—does this information make sense? Authenticate the individual and business Leverage data to customize fraud risk scores where moderate to high volumes exist online Educate your team at least twice a year on emerging tactics and techniques fraudsters are using—share examples, participate in fraud professional workshops Adopt an all-eyes approach—implement a "TIPS" line to encourage all employees to identify and report potential frauds
Detection and inspection	Create a rules engine to automate and review portfolio for patterns, velocity and outliers—which may require further inspection Set up email or phone notifications of customer changes Build relationships—share cases with appropriate parties (i.e., U.S. Secret Service, FBI, state and local police, Secretary of State) Investigate and actively work with law enforcement to prosecute cases
Recovery and Learning	Evaluate your entire customer portfolio and benchmark your "true" fraud loss exposure ■ Most risk lies with existing accounts ■ What types/portion of first payment default is fraud Develop executive dashboard for easy tracking and reporting Learn and adapt from past instances of deception ■ Develop your own "Hot Data Files" of bad company names, hot addresses, suspect principal names, suspect registered agent names, heavy loss zip codes or counties and first time payment defaults Communicate successes to deter future fraudulent attempts Collaborate and share learnings across peer network—and create a clearinghouse of fraudulent activity and patterns Support prosecutions