Identifying small-business fraud

Not seeing the whole picture can hurt your bottom line

An Experian white paper

Identifying small-business fraud

Executive summary

Among fraud topics, small-business fraud and the challenges organizations face in identifying and mitigating these losses frequently are overlooked and are not well-understood. Small-business fraud is not as visible as consumer fraud because businesses often are not seen as victims in the way that consumers are. With no legislation requiring fraud to be reported and no national bodies to collate information, there is a dearth of information on which to base statistics.

The statistics that are available indicate that business fraud losses are staggering in scope and are increasing. According to a 2007 Javelin Strategy & Research study, fraud-related costs for U.S. businesses are more than $50 billion annually. This figure may understate the extent of the problem, as estimates show that up to 30 percent of all bad-debt commercial losses are due to "soft" fraud, which primarily occurs from material misrepresentation on an application. Combined with the fact that business fraud is estimated to be three to 10 times more profitable than consumer fraud, business fraud has become a growing concern for organizations.

"The industry click fraud rate climbed to 17.1% in the last quarter of 2008, up from 16.6% one year earlier. The increase represents the highest level recorded since rates started being tracked in 2006."

Source: Click Forensics

"The number of identity fraud incidents increased by 22 percent over 2007, which brings them back up to levels not seen since 2004. One significant factor likely contributing to this rise is economic misfortune."

Source: Javelin Strategy & Research 2009 Identity Fraud Report

"The number of data breaches reported in 2008 increased by 47 percent over 2007."

Source: Identity Theft Resource Center

"In 2008 an estimated $4 billion in online merchant revenues were lost to payment fraud, up from $3.6 billion in 2007."

Source: CyberSource 2009 Online Fraud Report

Experian® addresses the factors contributing to small-business fraud today and offers best practices that focus on combining business and consumer data with analytics. Through analysis across various portfolios, Experian developed business, consumer and blended scores and analyzed their performance to improve the identification of potential small-business identity fraud.

Identifying small-business fraud

The current small-business fraud environment

To understand the depth of today's small-business fraud problem, we must consider the correlation between weakened economic conditions and the rise in fraud attempts. Historically, during periods of economic misfortune, higher rates of fraud occur. Individuals under extreme financial pressure are more likely to resort to desperate measures, such as misstating financial information on an application to obtain credit. Additionally, seasoned fraudsters take advantage of economic turmoil and anxiety by exploiting consumers and businesses through various methods. For example, with the recent mergers and acquisitions among financial institutions, industry experts are seeing a rise in "phishing," a practice in which fraudsters send fake e-mails that appear to originate from the acquiring financial institution in order to obtain the account holder's information.

Not only are fraudulent attempts on the rise, but support from law enforcement in investigating fraud cases and recovering money for business victims is diminishing. U.S. Justice Department data, which includes cases from other agencies such as the Secret Service and The Postal Service,® show that prosecutions of frauds against financial institutions dropped 48 percent from 2000 to 2007. This decrease primarily resulted from shifting law-enforcement resources from criminal investigative work to expanded national security efforts after the 9/11 attacks.[1]

Additionally, victimized businesses often aren't afforded the protections that consumers receive under identity theft laws, such as access to credit information. For example, prior to California recently amending its 1997 identity theft law to include crimes targeting business identities, a business whose identity had been stolen could not even file a police report. "We were having businesses being taken over and their names being used, and I could not prosecute them, at least [not] under identity theft statutes," California Deputy Attorney General Robert Morgester stated. Moreover, Morgester said some detectives have 50 identity theft cases on their desk at any given time, and they must focus on the handful where they think they can make an arrest and get a conviction. If the loss is relatively small — under $10,000, he suggested — police may be reluctant to take it on. At the federal level, some U.S. attorneys have thresholds of $1 million. In addition, even though the average victimized business has greater losses than the average individual consumer victim, crimes against businesses continue to be commonly viewed as "victimless crimes" and therefore receive less focus than consumer cases.[2]

Small-business fraud types

Small businesses face a myriad of both first- and third-party fraud behaviors, varying significantly in frequency, severity and complexity. A first-party, or victimless, profile is characterized by having some form of material misrepresentation — for example, misstating revenue figures on the application — by the business owner without the intent or immediate capability to pay the loan item. A third-party profile, or one in which a victim is involved, is characterized by a third party stealing the identification details of a known business or business owner in order to open credit in the victim's name. Some of the most prevalent types of small-business fraud affecting organizations across multiple industries are discussed on the next page.

[1] *Source: http://www.businessweek.com/smallbiz/content/jul2007/sb20070723_261131.htm*

[2] *Source: http://www.businessweek.com/smallbiz/content/jul2007/sb20070723_261131.htm*

Never payment

Never payment, also known as "never pay," occurs when an individual or a business opens a new account and never makes a single payment on any debt owed. Some organizations consider this behavior to be a credit risk problem, while others consider it to be a fraud problem. Regardless of how it's classified, never-pay losses are rising, and creditors are becoming concerned about its prevalence. Never-pay behavior can be classified as either first-party or third-party fraud. With first-party never pay, the individual provides some form of material misrepresentation to obtain a loan but has no intention of paying. A third-party never pay is perpetrated when a third party steals the identification details of the business owner or business in order to open a loan or an account in the business's name and never makes a payment on the debt. Most creditors currently do not have a reliable method of identifying never-pay accounts. As a result, these accounts often are treated as traditional credit losses and written off as bad debt. Given the uncertainties in today's economic environment, organizations must have a way to predict never-pay behavior and prevent future losses.

Example: A small-business card provider received a new business card application. Unknown to the provider, the account holder falsified financial information on the application. The credit line was issued in accordance with information from the application. The customer did not make the first payment on time or within the defined grace period and subsequently never made any payments. After the loss, the provider discovered the falsified financial information and classified the loss as a fraud loss instead of a credit loss.

Shell companies

Shell companies are characterized as fictitious entities created for the sole purpose of committing fraud. They often provide a convenient method for money laundering because they are easy and inexpensive to form and operate. These companies typically do not have a physical presence, although some may set up a storefront. According to the U.S. Department of the Treasury's Financial Crimes Enforcement Network, shell companies may even purchase corporate office "service packages" in order to appear to have established a more significant local presence. These packages often include a state business license, a local street address, an office that is staffed during business hours, a local telephone listing with a receptionist and 24-hour personalized voice mail.

Example: In one recent scenario, a shell company operated out of an office building and signed up for service with a Voice over Internet Protocol (VoIP) provider. While the VoIP provider typically conducts on-site visits to all new accounts, this step was skipped because the account was acquired through a channel partner. During the first two months, the account maintained usage patterns that were normal for the account's profile, and invoices were paid promptly. In the third month, the account's international toll activity spiked, causing the provider to question the unusual account activity. The customer responded with a seemingly legitimate business explanation of activity and offered additional documentation. The following month, the account contact and business disappeared, leaving the VoIP provider with a $60,000 loss. A follow-up visit to the business showed a vacant office suite. Further, postloss account review through Experian's Commercial Fraud Insight℠ identified 12 businesses listed at the same address, suggesting that the perpetrator set up these businesses and victimized multiple organizations.

Identifying small-business fraud

Business identity theft

In business identity theft scenarios, the perpetrator acts as the business owner or representative of a legitimate company, commonly through the use of false company letterhead and contact details, to obtain credit in the existing company's name. (This type of fraud differs from consumer identity theft, in which an individual's personal information is compromised in order to obtain credit in that individual's name.) Accounts are opened in the name of the reputable company, and goods are sold and often collected by the person(s) pretending to represent that company.

Example: The perpetrator, ABC Company, leased a space in the same building as XYZ Company and then applied for credit under XYZ's name. XYZ's business name matched with the correct address, so the application passed the credit check. Credit cards were delivered to the perpetrator's mailbox at the same address. The perpetrator then vanished and most likely sold the cards on the street. This is a common scenario because many organizations still rely only on credit information alone and do not conduct business verification checks or use multiple data sources in the application process.

Account takeover

Account takeover is when a fraudster compromises an existing account established by the legitimate business. It is likely to increase at a higher rate than other fraud types because of current economic conditions. Frauds of this kind are enabled through e-mail (phishing) and telephone scams. They also are accomplished through the interception of credit cards and statements in order to take over an account, divert or fraudulently order goods, or facilitate fraudulent transactions. As creditors become more and more stringent with credit-granting policies on new accounts, application fraud is less likely to be successful, potentially resulting in perpetrators shifting their focus to taking over existing accounts. The Credit Industry Fraud Avoidance System (CIFAS), a nonprofit fraud prevention association in the United Kingdom, recently reported that account takeover fraud showed the most significant growth of any fraud category in 2008, resulting in an unprecedented 207 percent year-over-year increase. Industry experts predict that U.S. account takeover fraud trends will be consistent with CIFAS' report.

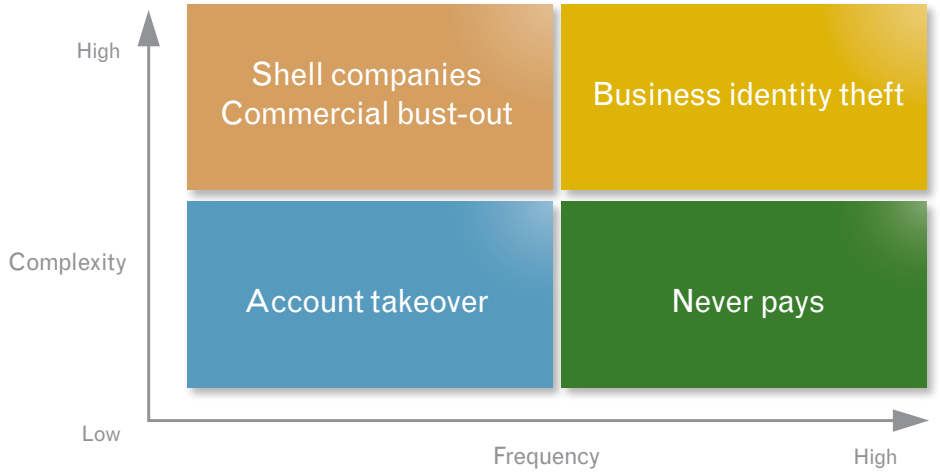
Example: A small-business card provider detected a cardholder's attempt to make an online airfare purchase to a remote country. (This type of purchase tends to carry a high rate of fraud.) The IP address, a unique Internet access address identifier for each individual online computer, revealed that the online purchase had originated in the Philippines. Because the California-based cardholder had made no previous purchases outside the United States, the provider was alerted to possible fraud. U.S.-based transactions within the account's normal activity were occurring simultaneously with the fraudulent charges, indicating that one set of charges was not legitimate. Further review showed that multiple online "test transactions" in small dollar amounts had occurred several days earlier. These test transactions are a common practice by fraudsters to determine if the transactions will be rejected or approved. The purchase attempt was later confirmed as fraudulent by the cardholder, who also disclosed that her laptop recently had been receiving malicious software warnings. The perpetrator likely compromised the account by hacking into the cardholder's laptop and, by capturing keystrokes, stole the cardholder's information.

Commercial bust-out

A bust-out is a fraud tactic where the fraudster opens many lines of credit and eventually abandons all accounts after maxing out or exceeding all the credit lines. Bust-out equates to millions of dollars in losses and comprises a huge percentage of bad debts. In commercial bust-out schemes, fraudsters typically establish an account to obtain credit, build good history with the issuer and request credit line increases in the months prior to bust-out. They then write a bad check that puts them at or above their original credit limit. They take advantage of the "float" time between issuing the check and the attempt to clear it. Bust-out schemes often will utilize 100 percent to 200 percent of the original credit line, resulting in high dollar losses per account. Although bust-out accounts make up a significant percentage of issuer losses, they often are difficult to quantify because they are misclassified as credit loss rather than fraud.

Example: In a recent commercial bust-out, the perpetrator used the identity of a recently sold business. Leveraging the established credit history of the small business, the fraudster ran the credit line up to the limit, which amounted in a $27,000 loss.

Fraud risk exposure quadrant



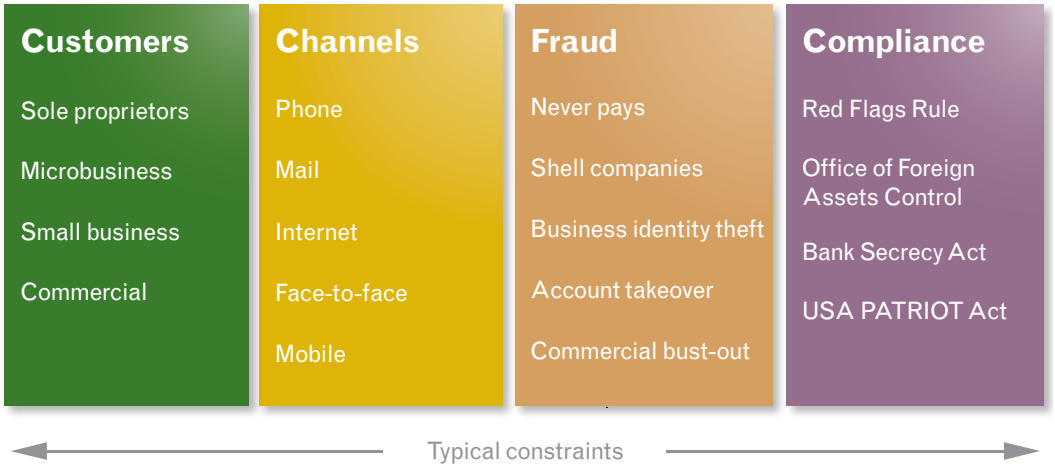
Challenges faced in identifying small-business fraud

Creditors face multiple challenges in identifying small-business fraud. Their first and most critical challenge is making sure that the underlying data sources used to check an applicant's information are reliable. Creditors often unknowingly rely on self-reported data, such as corporate filings and public records. Fraudsters can easily submit the paperwork necessary to obtain these filings and records, so creditors should be concerned about the quality of this public record data. There are numerous Web sites that can assist an individual in setting up a business entity, often preparing and filing articles of incorporation on the applicant's behalf. Proof of the officer's identity may not be required, and validation of the company's address is not conducted. The typical information required by secretaries of states' offices includes company

name; number or type of shares (if incorporated); names, addresses, or signatures of incorporators or organizers; and filing fees. These offices check for the availability of the desired company name, make sure all required information has been provided and process the payment for the application. Information collected from applicants is not verified. The process from application to acceptance, suspension or rejection can take from five minutes to 60 days.

Capturing business and business owner information

The amount of applicant information available for verification may be limited due to thin organizational application requirements. Many lending organizations do not require both business and business owner information from small-business applicants. Often, even if both sets of information are captured, the organization may not verify both sets of data because there is a perception that verifying both sets of information is unnecessary and/or increases manual review time and costs. Consequently, this perception results in missed high-risk alerts. Suppose a perpetrator steals a business's identity and has the real business's name, address, phone number, tax identification and (seemingly) accurate business documentation. The application is processed and approved because only the business-related information is verified. Conversely, the creditor requesting additional applicant information (business owner name, address, phone number and Social Security number) may confirm the applicant as a high fraud risk.



Compliance requirements

Organizations also face increased challenges to comply with various government regulations such as the Red Flags Rule, the USA PATRIOT Act mandates related to Office of Foreign Assets Control (OFAC) checks, and Customer Identification Programs without incurring increased costs or customer inconvenience. Holders of small-business accounts often ask if these accounts fall under Red Flags Rule enforcement, which applies to any financial institution or creditor that maintains accounts. Under these rules, a "covered account" is defined as a consumer credit account or a consumer deposit account involving multiple payments or transactions. Commercial credit and deposit accounts also can be included as covered accounts

when there is a "reasonably foreseeable risk" of identity theft to customers or to the safety and soundness of the account holder. To determine if there is a reasonably foreseeable risk of identity theft in a business or commercial account, consider the risk of identity theft presented by the methods used to open business accounts, the methods provided to access business accounts and previous experiences with identity theft on a business account. Financial institutions offering small-business credit should consult their legal counsel or federal regulators to verify that their compliance program and procedures are suitable for each account type. Nonfinancial institutions also face increased due-diligence efforts and should seek advice from their legal counsel for compliance program standards. Trade organizations are often good sources of information about how regulations apply to specific industries.

Best practices to reduce small-business fraud

The compliance landscape, along with customers' demands for "instant" services, drives organizations to automate processing and decisioning systems to maximize approval rates and control risks.

Incorporating the following best practices can reduce both the frequency and the severity of small-business fraud losses:

- **Start simple: Verify basic contact information of the business and business owner**
  Analysis of known business fraud records conducted by Experian's Decision Analytics team indicated that a sizable portion of small-business fraud can be identified through simple demographic verification. At the time of application, 59.4 percent of the known fraud records showed that the business address provided was invalid, not associated with the business or a vacant property. Analysis of the business owners' residential addresses showed that 48.5 percent of the fraud record addresses were invalid, not associated with the owner or a vacant property. The

Identifying small-business fraud

phone data showed that 8.7 percent of the businesses and 21.4 percent of the business owners were either invalid phone numbers or not affiliated with the business or business owner. Analysis of the business owners' Social Security numbers showed that 8.7 percent of the fraud records with Social Security numbers belonged to a deceased individual, were never issued or were not affiliated with the individual.

- **Identify repeat offenders**
  Individuals who commit fraud are commonly repeat offenders who serve little or no jail time. Less-sophisticated perpetrators are providing the same business-related information (business owner name, address, phone, tax identification number or Social Security number) multiple times. Why would a fraudster go through the effort of using another stolen Social Security number if the same one has worked multiple times? The simplest way for an organization to detect known fraudsters is to check the applicant and application details against internal and external known frauds.

Repeat-offender scenario

Applicant 1	Applicant 2	Applicant 3	Applicant 4
Business: C Gull Inc. 761 E. Green St. Orange, CA 91101 1 714 356 4567 Business principal: Randall Scandal 208 Fox Lane Anaheim, CA 92360 714 545 6825	Business: GL Trucking 222 South Ave. Tustin, CA 92654 1 714 356 4567 Business principal: Terry James 4556 Terrance Ave. Orange, CA 91102 714 798 7800	Business: GL Color Inc. 761 E. Green St. Orange, CA 91101 1 714 546 4785 Business principal: Betty Barnes 4006 38th Ave. Orange, CA 91102 714 545 9892	Business: WT LLC 317 Centre Ave. Orange, CA 91101 1 714 212 6865 Business principal: Terry James 208 Fox Lane Anaheim, CA 92360 714 545 6825

Recent Experian analysis illustrated the benefits of checking historical data within an organization. Doing so allowed organizations to detect up to 55 percent of fraud. Moreover, those organizations that share data and cross-match across the industry detect up to 70 percent more fraud. Industrywide negative databases, such as Experian's National Fraud Database,℠ enable members to share confirmed fraud records through reciprocal reporting. Many organizations opt to check new applications against their own negative data through an internally or externally hosted database. Organizations challenged with constrained IT resources or those with limited experience with hosting a negative database often utilize an external provider to host their data and integrate the check within their application processing environment.

Through the use of Experian's Commercial Fraud Insight historical matching capabilities, one payment processor identified multiple repeat offenders within the first week of implementation. A telecommunications provider achieved significant loss reduction in a geographical region primarily through identifying repeat offenders. As small-business authentication tools become more widespread and more creditors incorporate historical application checks, it is anticipated that repeat offender activity will decrease, causing fraudsters to come up with new schemes and tactics.

- **Analyze processes across all channels**
  The example we presented earlier in the paper in which the VoIP opened a business account through a channel partner and later discovered authentication steps were not carried out thoroughly underscores the need for possible further action against fraud. Organizations may need to implement additional risk-mitigation efforts in delivery channels that are not face to face, such as call centers or online purchasing vehicles. In an Experian study involving a group of U.S. retail card issuers, fraud rates were analyzed and compared with channel size. The study indicated that Internet applications were more than four times the fraud rate of other channels. Preliminary findings in small-business lending also indicate the higher rates of fraud in "faceless" channels such as the Internet.

	Mail	Point of sale	**Internet**
Percentages of applications	9.00%	85.00%	**6.00%**
Fraud rate	0.14%	0.06%	**0.79%**

While the smallest channel in volume, Internet applications equate to more than four times the fraud rate of other channels.

- **Smart decisioning through analytics**
  Nearly every organization faces the need to balance cost-reduction efforts while continuing to book profitable customers. The pervasive theme across multiple industries is to do more with fewer resources. One common approach to managing customer acquisition costs is incorporating automated decisioning through targeted analytics. By using analytics to separate suspect businesses and business owners from those that don't exhibit characteristics of fraud, creditors can more effectively allocate analyst resources, simplify customer treatment and set fraud risk tolerance levels.

  Implementing a score-based approach not only reduces operational costs by lessening manual efforts, but it also helps mitigate false positives and improves the customer experience by reducing the impact of manual reviews of good customers. Experian has spoken to and listened to key clients who have stated that the key to preventing small-business fraud is through blending business and consumer data. As a result, Experian has decided to analyze the associated lift, utilizing vast data assets on both the consumer and commercial sides. Later this year, we will release our BizID℠ product, which leverages Experian's leading consumer product, Precise ID℠ (used by five of the top seven U.S. financial institutions), and Experian's leading commercial tool, Commercial Fraud Insight. BizID will help clients to streamline business application authentication by verifying and validating business and business owner data through one service and will assist clients in decisioning through the use of custom or generic business, business owner and blended fraud scores.

Identifying small-business fraud

A debate regarding combating small-business fraud exists among organizations: Is blended data always better? The answer is twofold. Verifying business and business owner data always is better than verifying one data set. Failure to do so could result in a missed OFAC hit on the business or a Social Security number belonging to a deceased individual being used by the business owner. From a scoring perspective, using a score that leverages consumer and business data is the best approach but is not always possible with sole proprietors or new small businesses. Overall, the best approach is to verify as much information as possible (business and business owner data) and implement a tool that intuitively returns a score that is most predictive of fraud at the individual-application level.

Conclusion

Business-to-business fraud is increasing, and fraudulent attempts vary significantly in complexity and approach. Fraud is prevented because fraud is detected. Verifying that the business and business owners are who they say they are using multiple data sources is critical to identifying applicant irregularities. Experian is committed to listening to client needs and producing solutions, such as BizID, that mitigate small-business fraud through delivering quality data, targeted analytics and blended decisioning. A well-executed fraud strategy can improve fraud identification and operational efficiency, thereby reducing small-business customer acquisition costs.

To find out more about small-business fraud, contact your local Experian account representative or call 1 888 414 1120.

Experian
475 Anton Blvd.
Costa Mesa, CA 92626
1 888 414 1120
www.experian.com

03/09 • **2000/1054** • 5013-CS