White Paper

Business Risk Information: The Need for Clearer, More Comprehensive Intelligence on Businesses and People Associated with them

Strong business decisions begin with deeper insight into the companies and people you do business with

Credit Risk Decisioning, Compliance and Fraud

LexisNexis®

Summary

Financial institutions are seeking to expand the universe of prospects, but competition is fierce. One way to differentiate themselves is by going after prospects that others are not. Small and new businesses, which can be very profitable, present a great opportunity to do this. Small businesses have historically been under-targeted because they are difficult to "find," and they represent riskier investments. LexisNexis addresses these issues through coverage of more small businesses, and linkages to information about the people behind the business which is often the best indicator of a small business' risk profile. Its superior coverage also helps to streamline verification, as part of the due diligence process.

Criminals use businesses to mask their activities. Shell companies, generally defined as business entities without active business or significant assets, have been abused for money laundering and terrorist financing. When shell companies are set up by mass incorporators (business set up with the sole purpose of setting up and selling shell companies), authorities have no way of knowing the true ownership of the company. Financial institutions can combat the activities of mass incorporators by screening for things such as, "Does this business addresses have an unusual number of businesses registered to it?"

Identity fraud is not just a crime committed against consumers—businesses present prime targets as well. In fact, identity thieves are increasingly targeting businesses. Better verification and authentication of applicant and customer identities can help to prevent business identity fraud.

Credit Risk Decisioning – Uncover Hidden "Gems" through Better Coverage of Small and New Businesses

With the lending industry projected to grow at an annual compounded rate of 6 percent between 2014 and 2018,[i] financial institutions are under pressure to boost customer acquisition in order to keep pace with the market. Because of fierce competition for new customers, financial institutions have increased the volume of marketing campaigns significantly in recent years. As a result, response rates have plummeted: the Direct Marketing Association reports that direct mail response rates have dropped 25% over the past nine years, with similar decreases across other marketing channels.[ii]

Targeting new and small businesses presents a great opportunity to outflank the competition and target customers that others are not. Small businesses can be very attractive customers: an Oliver Wyman analysis conducted for LexisNexis suggests that small businesses account for 40% of lending profit at US banks. Newer businesses are particularly attractive because they are typically in the market for lending services.

Small and new businesses have historically been under-targeted is because they are difficult to "find." They also tend to be more risky—less than half of small businesses survive for five years[iii]. LexisNexis helps to address these issues through coverage of more new and small businesses, and information about the people behind the business which is particularly relevant for ascertaining small business risk. Its superior coverage also helps to streamline verification, boosting the efficiency of the due diligence process.

Compliance – Combat the Abuse of Shell Companies for Money Laundering & Terrorist Financing

Shell companies are generally defined as business entities with no active business, employees or significant assets. They can have legitimate purposes. For example, a public figure may use one to hold his home, in order to protect his family's privacy. However, shell companies can also be abused. According to a 2009 special alert from the Federal Deposit Insurance Corporation (FDIC): "[Shell] companies are often formed by individuals and businesses to conduct legitimate business transactions. However, they can be and have been used as vehicles for common financial crime schemes such as money laundering...By virtue of the ease of formation and the absence of ownership disclosure requirements, [shell] companies are an attractive vehicle for those seeking to conduct illicit activity." [iv]

There have been several high-profile examples of abuse of shell companies in recent years. In 2010, Florida attorney Scott Rothstein pled guilty to fraud and money laundering in connection with a $1.2B Ponzi investment scheme, in which he used 85 US shell companies to conceal his participation or ownership stake in various real estate and business ventures.[v] In 2011, Victor Kaganov, a former Russian military officer who ran an illegal money transmitter business from his home in Oregon, pled guilty to using Oregon shell companies to wire more than $150M to other countries on behalf of Russian clients.[vi]

States require someone to act as the business "owner" or legal representative during the initial filing of a company[vii], and banks also require an "owner" during the account set-up process. Therefore, individuals who do not wish to have their identities associated with a business need to find someone else who is willing to set up the business and business banking account. Scores of mass incorporators, whose sole purpose is to set up and sell "shelf" companies (a variety of shell company that has been set up and put "on the shelf" to age), have stepped in to fill this need. These mass incorporators have hundreds or even thousands of companies for sale at any given time.

Historically, the hotbeds of the mass incorporator industry have been three states with a light regulatory touch – Delaware, Wyoming and Nevada. A Delaware-registered company may be owned by a national of any jurisdiction, regardless of his or her place of residence. The company can be operated and managed worldwide, and it is not required to report any assets.[viii] And Delaware is not even the most permissive US jurisdiction with regard to company formation. Wyoming and Nevada allow the real owners of corporations to hide behind "nominee" officers and directors with no direct role in the business, often executives of the mass incorporator.[ix] "Somalia has slightly higher standards than Wyoming and Nevada," says Jason Sharman, a professor at Griffith University in Nathan, Australia, who prepared a report for the World Bank on corporate formation worldwide.[x]

In June 2011, Reuters published a special report on the mass incorporator industry which profiled a firm known as Wyoming Corporate Services. The Wyoming Corporate Services website stated: "A corporation is a legal person created by state statute that can be used as a fall guy, a servant, a good friend or a decoy. A person you control...yet cannot be held accountable for its actions. Imagine the possibilities!"

According to the report, over two thousand companies set up by Wyoming Corporate Services were registered to a single address in Cheyenne, Wyoming. These companies included:

- a corporation controlled by former Ukrainian Prime Minister Pavlo Lazarenko, convicted of money laundering and extortion
- a corporation indicted for helping online-poker operators evade a US ban on Internet gambling
- two corporations barred from US federal contracting for selling counterfeit truck parts to the Pentagon

In August 2011, Senators Carl Levin (D-MI) and Charles Grassley (R-IA) introduced the Incorporation Transparency and Law Enforcement Assistance Act. This bill would have required states to obtain and update information about the real owners of companies, and it would have imposed civil and criminal sanctions for filing false information.

The information collected would have been made available to law enforcement through a subpoena or summons. The bill was allegedly killed by a coalition of state officials and business groups who cited concerns about the cost of implementing the new law and federal government infringement on state incorporation rights.[xi]

LexisNexis can help to combat the use of shell companies for money laundering and terrorist financing. It does this by helping financial institutions know more about new and existing business customers. Indicators of high risk can include business addresses at which an unusual number of businesses are registered[xii], or business owners who "own" or are the registered agent for an usual number of businesses. Lower risk businesses, on the other hand, tend to be set up in states that promote transparency about ownership and to have an owner who is only associated with one business. Streamlined access to this information is helpful to financial institutions to "clear" these lower-risk businesses expeditiously.

Fraud – Deter Business Identity Fraud through Verification and Authentication

Just like consumers, businesses have identities that can be stolen. In fact, businesses make attractive identity fraud targets for a number of reasons:

1. **Businesses usually have larger bank account balances and credit limits, compared to consumers.**
   Analysts report that it is not unusual for business identity fraud losses to be in the mid-six figures by the time the criminal activity is detected.[xiii]

2. **Sensitive information about businesses is often easily accessible.**
   In most states, businesses are required to dutifully post documents that contain many of their key identifiers (e.g. sales tax number, business license number), and business credit reports containing a wealth of information about the business can be ordered by virtually anyone.

3. **Identity fraud laws, as currently written, apply mostly to consumers rather than businesses.**
   Federal law and many state laws classify identity fraud only against individuals, hindering the efforts of investigators and prosecutors in the cases where a business' identity is stolen. "Identity thieves increasingly target businesses instead of individuals, experts and law enforcement officials say, but federal law and many state statutes don't consider business identity theft a crime. That's because the raft of identity theft laws passed....apply mostly to individual consumers—not business entities."[xiv]

4. **There is lesser likelihood of transaction anomalies in business accounts being detected by financial** institutions' fraud detection systems.
   Most of these systems have been designed and calibrated to detect fraud perpetrated against consumers, rather than businesses.

As a result of these factors, business identity fraud has proliferated in recent years. In fact, industry research has found that 9% of small businesses have experienced identity fraud.[xv] LexisNexis can help to combat business identity theft through verification and authentication to prevent the two most common types of identity fraud:

Type of Identity Fraud	LexisNexis Solution
Identity Theft A fraudster uses the business' identity to set up a new account. For example, he may obtain credit in an existing company's name by acting as the owner or representative of that company, commonly through use of false company letterhead and contact details.	Industry analysis of known fraudulent applications found that over half had provided a business address that was invalid or not associated with the business and that more than 20% of business "owners" provided a phone number that was invalid or not associated with the owner.[xvi] Using LexisNexis InstantID® to verify information provided at account set-up can prevent the approval of these fraudulent applications.
Account Takeover A fraudster gains access to an existing business account. He may steal an account statement from the mail in order to get an account number. Then he may search online to gather information about the business that can be used to convince a customer service rep to grant him access to the business' account. Account Takeover is facilitated by the fact that many financial institutions have traditionally required minimal business owner / representative information from small business customers, so there is little information on file to indicate who is authorized to access the account.	Customers can establish that individuals seeking access to a business account should actually be granted access by using LexisNexis InstantID® Q&A to ask the individual questions about the business that only an owner or financial officer could typically answer.

Sources

[i] First Research, February 2014

[ii] Direct Marketing Association, 2014

[iii] "Startup Failure Rates – the Real Numbers," 2008

[iv] "FDIC Special Alert," 4/24/09

[v] "Scott Rothstein Charging Document," Scribd.com, 12/2/09

[vi] "Oregon Man Pleads Guilty to Operating Illegal Money Transmitting Business That Moved More Than $172 Million Through Shell Corporations in the United States," Department of Justice Office of Public Affairs, 3/1/11 . This is a small slice of the $36B billion that the FBI believes US shell companies and bank accounts are being used to launder from the former Soviet Union. "US Money Laundering Threat Assessment," working group of members from the Department of Treasury, Department of Justice, Department of Homeland Security, Board of Governors of the Federal Reserve, and US Postal Service, December 2005

[vii] State Business Entity Law Summary," National Association of Secretaries of State, 5/13/09.

[viii] "US Money Laundering Threat Assessment," working group of members from the Department of Treasury, Department of Justice, Department of Homeland Security, Board of Governors of the Federal Reserve, and US Postal Service, December 2005. The report form this working group stated, "The competition among certain states to attract legal entities to their jurisdictions has created a 'race to the bottom' and a real money laundering threat."

[ix] "State Business Entity Law Summary," National Association of Secretaries of State, 5/13/09.

Note that some attorneys with loose ethics will even create a company on behalf of clients so that they can invoke attorney-client privilege if there is ever question about the ownership of the company.

Also note that LLCs are particularly prone to abuse, as they make it particularly easy to mask ownership. Because of this, the Treasury Department has singled out LLCs as being particularly vulnerable to money laundering. Each state in the US has its own unique business entity formation statutes. Only four states – Alabama, Alaska, Arizona and Kansas – require LLCs to report their members regardless of the existence managers. 14 states, on the other hand, impose no requirement to report the identities of either managers or members. Those 14 states are Arkansas, Colorado, Delaware, Indiana, Iowa, Maryland, Michigan, Mississippi, Missouri, New York, Ohio, Oklahoma, Pennsylvania, and Virginia. "The Role of Domestic Shell Companies in Financial Crime and Money Laundering: Limited Liability Companies," Department of the Treasury Financial Crimes Enforcement Network, November 2006. The popularity of LLCs has grown in recent years, currently representing more than half of US partnerships. "Partnership Returns, 2006," IRS Statistics of Income Bulletin, Fall 2008

[x] "Special Report: A little house of secrets on the Great Plains," Reuters, 6/28/11

[xi] "Special Report: A little house of secrets on the Great Plains," Reuters, 6/28/11

[xii] In Wilmington, Delaware, one specific address serves as headquarters for over 200,000 companies. "It's time to pry criminals out of their shell (companies)," cleveland.com, 8/16/13

[xiii] *The Consumer Identity Theft Protection Manual*, 2010

[xiv] "Identity Theft: The Business Bust-Out," *Bloomberg Businessweek*, 7/23/07) Note that these crimes can often be prosecuted under other lesser charges, like mail fraud or wire fraud.

[xv] "2012 Identity Fraud for Small Business Owners," Javelin Strategy & Research

[xvi] "Identifying small-business fraud," Experian, 2009

For More Information

Call 866.277.8407
lexisnexis.com/risk

About LexisNexis® Risk Solutions
LexisNexis® Risk Solutions (www.lexisnexis.com/risk/)is a leader in providing essential information that helps customers across all industries and government predict, assess and manage risk. Combining cutting-edge technology, unique data and advanced scoring analytics, Risk Solutions provides products and services that address evolving client needs in the risk sector while upholding the highest standards of security and privacy. LexisNexis Risk Solutions is part of Reed Elsevier, a leading publisher and information provider that serves customers in more than 100 countries with more than 30,000 employees worldwide.

LexisNexis®