Managing Risk in the Moving & Storage Industry

ISSUE 02

The Dispatch

MOVER'S CHOICE BRIEFINGS

Article Written By:
Matt Schiefferly

Matt Schiefferly, Principal, Paul Hanson Partners

Matt Schiefferly attended UC Davis where he studied Economics and Political Science. Matt has been a producer at Paul Hanson for 15+ years specializing in insurance placement and consulting for moving and storage companies. Matt has also been the director of Safety and Loss Control at Paul Hanson and has consulted with transportation companies and associations across the country on loss control, safety and risk management topics.

This article is informational only.

Identity Theft - Not Just a Crime Against Consumers

Identity theft is not just a crime against individual consumers. Criminals have learned that unsuspecting businesses also are viable targets for identity theft. It's called business identity theft or business identity fraud and occurs when your business identifying information is used fraudulently by an imposter.

Can this happen to your moving and storage company?

Well, in 2014, the American Moving & Storage Association alerted members to a warning from the Federal Motor Carrier Safety Administration about business identity theft reaching the transportation industry. They cited company websites being hijacked, illegal use of USDOT or MC numbers, former employees using company marked property, and use of decommissioned equipment still bearing the former company's name or logo.

Criminals are finding many ways to steal a business's identity, often manipulating and falsifying business filings and records. Their goal is to defraud a business's creditors and suppliers, financial institutions, business' owners and officers, unsuspecting consumers and even the government.

Common Schemes

One common scheme is fraudulent business registration and filing. In many states, it is easy for thieves to manipulate online state business registration systems and filing processes. They impersonate a business, establish themselves as officers and then deceive retailers, suppliers, creditors, financial institutions or other businesses for illicit gain.

Another scheme is called physical address mirroring. After criminals gain information about a company's finances, credit, suppliers, owners and officers, they rent space in the same office building as their target company. This allows them to exploit weaknesses in address-based verification, authentication and fraud detection systems to apply for credit cards, loans and lines of credit in the business' name.

Phishing scams are also popular. In these cases, fraudsters send emails in the business' name, hijacking or counterfeiting their email. They spam or “spear” phish email to the business' clients, tricking them into divulging confidential personal and business account infor-mation, including an EIN, social security number, user name and password. Or worse, they trick them into remitting payments to a fraudulent location. Many of us are familiar with these deceptive emails to our personal accounts, but they are a common, serious and often effective form of business identity theft as well.

These are just a few of many business identity theft schemes, and the impact on the target business can be significant.

Identity Theft - Not Just a Crime Against Consumers

Criminals get into your bank records to withdraw or spend funds, sometimes using wire transfers and electronic transactions. They may set up credit accounts in your name and engage in activity that damages your credit. And, of course, they can harm your reputation.

Prevention

With so much at stake, businesses should take proactive steps to monitor their business activity and flag illegal activity before it goes to far.

Prevention begins with putting best practices in place to secure your bank accounts, credit and customer records:

- Talk to your bank about implementing security and authentication controls to protect against illegal wire transfers and electronic transactions.
- Monitor and reconcile your business accounts daily through online banking.
- Carefully review and reconcile account statements a s soon as they are received, and ask trade and credit references to notify you if they are contacted.

Secure and protect all business and financial information:

- Protect your business EIN as you would your own Social Security number.
- Store all documents in a secure location and shred old documents.
- Protect and monitor your state business registration information.
- Review business credit reports, and keep business and personal information separate.

Secure your computer systems:

- Install and use regularly updated anti-virus, anti-spyware and/or Internet security software, and keep security patches and software up-to-date.
- Use a firewall for your computer network and a password-protected wireless network.

- Be alert to web imposters: Criminals can use phony websites to deceive your clients into believing they are dealing with your business.
- Train all employees never to click on links in emails unless absolutely certain they are legitimate and secure.

Employees can function as your business's front-line defense. Educate your staff about security and privacy, emphasizing that sensitive company information is the responsibility of everyone in the organization. And train employees to recognize Phishing scams: Government agencies and financial institutions never request that you verify information through email communications.

Cover Yourself

If you are the victim of business identity theft, you will likely incur expenses to resolve the case. Business identity fraud protection programs that include insurance [Link to coverage page on Paul Hanson website] are intended to protect your business from various risks and the financial impact of business identity theft.

Insurance policies are designed to reimburse you for expenses incurred as a result of fraud, as well as efforts to remedy the fraud. These may include professional fees for defense of lawsuits or criminal allegations, removing civil or criminal judgments, contesting the inaccuracy or incompleteness of records containing your business information, and any necessary research, investigation or consulting. They also include lost wages and miscellaneous expenses.

Finally, take advantage of proactive tools and risk management services in these protection programs to help prevent identity theft.

Business identity theft can damage both your bottom line and your reputation. In fact, the stakes are much higher when compared with personal identity theft. But by taking necessary steps to monitor your finances, prevent illegal activity and cover your costs if you are a victim, you can better protect the business you have invested so much in.

DISCLAIMER: The information contained in this article has been developed from sources believed to be reliable. However, the accuracy and correctness of such materials has not been verified. We make no warranties either express or implied nor accept any legal responsibility for the correctness or completeness of this material. This information should not be construed as business, risk management or legal advice or legal opinion. Compliance with recommendations, if any, contained herein in no way guarantees the fulfillment of your obligations as may be required by any local, state or federal laws. Paul Hanson Partners assumes no responsibility for the discovery and/or elimination of relevant conditions in your operation(s) and/or facility(ies).