The Identity Theft Risk to Your Law Firm

by James Harrison, Founder and Chief Executive Officer, INVISUS

Most attorneys and legal management professionals are well aware of the identity theft epidemic. What they may not be sufficiently aware of is the risk to employees, partners and the firm itself. Business identity theft is big business for identity thieves — and it costs businesses billions every year in damages and lost productivity. Here's what you need to know.

YOUR FIRM ITSELF IS AT RISK

Criminals use Federal Employer Identification Numbers (EINs) and other publicly available information about businesses to open new lines of credit, mirror electronic payroll runs, redirect electronic funds transfers (EFTs), create bogus W-2 employee filings, and file fraudulent business tax returns.

Business identity theft is one of the fastest areas of growth in white-collar crime today. In July 2017, the IRS reported a 250 percent jump in business identity theft cases compared to the year before, with damages skyrocketing to $137 million during the six-month period.

A stolen business identity with a trail of fraud and crime can quickly destroy a company's reputation, credit rating and financial well-being. The risk here to your firm is no different than any other company. If your firm currently does not have a business identity theft protection plan, you should seriously consider it.

PARTNERS, STAKEHOLDERS ARE TARGETED

Your firm's partners and other key stakeholders or executives are at risk of having their personal information used to commit

> “As many as one in four people are currently dealing with banking, medical, tax return, Social Security, criminal record or other types of identity theft. This means 25 percent of your current staff is likely suffering with the financial, emotional and mental stress that comes with this crime.”

business fraud in your firm's name. Fraudsters can use a partner's or stakeholder's personal information to establish bogus credit accounts and act as a signatory or guarantor on leases, equipment purchases, investments, bank transfers and more — all big dollar business transactions that have the potential to hurt your firm.

When a business owner's or stakeholder's identity is stolen, it creates a direct risk to the business. These individuals need specialized protection against identity theft that includes coverage for business fraud. It is important to note that typical consumer identity theft protection plans do not cover business identity fraud problems.

1 IN 4 EMPLOYEES AFFECTED BY IDENTITY FRAUD

With the recent Equifax data breach alone, 147 million Americans had their Social Security number, date of birth, credit profile and other personal information exposed to the criminal underworld. Add to that the more than 15 million Americans who actually reported becoming victims of identity fraud in 2017 before the Equifax breach, and that means virtually all adults in the United States were impacted and could become victims of identity theft at some point in the future.

Several reports indicate that as many as one in four people are currently dealing with banking, medical, tax return, Social Security, criminal record or other types of identity theft. This means 25 percent of your current staff is likely suffering with the financial, emotional and mental stress that comes with this crime. Without proper monitoring and expert recovery help, the identity theft victim will spend seemingly endless hours and thousands of dollars fighting to defend her identity and clear her name.

PROTECT THE FIRM BY PROTECTING YOUR EMPLOYEES

An attorney or staff member who becomes a victim of identity theft can put the whole firm at risk. Today's cybercriminal can quickly leap from an individual to their family and then to their employer. Employees who are suffering from cybercrime and identity fraud at home can be a back door for the criminal into a much larger payday: your firm and your clients.

With so many people working from home and on the road and connecting through computers, smartphones and social media, protecting your employees is a smart layer of defense against the growing identity theft and cybercrime problem facing all businesses.

Data breaches, cybercrime and identity fraud are not going away anytime soon. Employers have begun offering identity protection to all personnel as an inexpensive way to protect the business — and as a hot new employee benefit. This employee perk has quickly become a part of the core benefits offered by businesses to provide security and peace of mind to current personnel. It's also become a great way to help attract and retain the best and brightest talent.

To protect your business, align your firm with a professional identity theft protection service that provides business entity coverage, specialized coverage for business owners and officers, and a solid employee benefit plan. In addition to robust monitoring and identity restoration services, be sure to look for programs that provide social media monitoring, and computer and mobile device security protections that round out a balanced identity theft protection strategy for your people and your business.

ABOUT THE AUTHOR

James Harrison the Founder and Chief Executive Officer of INVISUS. He is the market strategist and product visionary for INVISUS, responsible for the development of the company's identity theft, cybercrime, and information security compliance product lineup. As an industry expert, Harrison regularly speaks and trains at various industry and trade conferences including recent national conferences for ALA. INVISUS has partnered with ALA VIP℠ Cyber Risk Management Business Partner BreachPro to provide ALA member firms access to the iDefend and InfoSafe programs.

jami@invisus.com
www.breachpro.com