Key Takeaways from a Recent Employee Data Breach—The Biggest Threat May be Internal

By Carl Galant and Michael Kabat, Partners
September 24, 2015

Recently a former Morgan Stanley financial adviser pled guilty to criminal charges in New York federal court for allegedly stealing data from about 350,000 of Morgan Stanley's customers. This is the latest example of the increasingly common problem of a data breach compromising sensitive personal information and creating substantial risk for a business. It is also a reminder that businesses not only have to safeguard against hacking attempts by outsiders, but must also address the risk of data breach or theft by employees or others within the organization.

The consequences arising from a breach are expansive. Businesses that suffer a data breach face potential civil liability from customers whose sensitive personal information was compromised, particularly if the business failed to implement adequate safeguards and procedures to protect such information. If trade secret or proprietary information is stolen, the business may have to sue to enjoin the use of the stolen information and recover monetary damages. In certain situations, the Texas Attorney General can bring suit for civil penalties against businesses that fail to adequately safeguard sensitive personal information or fail to properly notify those affected by a breach. In addition to civil liability, there is the harm that comes from damage to reputation, disruption of business, and loss of business.

Not only must a business develop the procedures and infrastructure to prevent a breach, but the business must develop the procedures for responding to a breach. State and federal statutes mandate steps that must be taken to notify individuals who could be affected by a breach. Developing a breach response protocol before a breach occurs is critical to mitigating harm to affected individuals and your business.

Texas has a broad and demanding breach notification law. It applies to any business that maintains sensitive personal information, from retailers to small businesses with employee data. Any business or employer that maintains an individual's social security number, unique identification number, credit or debit card information, fi nancial information, or healthcare information should be cognizant of the risk of a data breach. Such events occur with disturbing regularity. The concern is not if a breach will occur, but when. The law requires that businesses be prepared. The key takeaways for any business are: (1) proactively develop policies, procedures, and network security infrastructure to safeguard against a breach; (2) include a breach response plan within your policies and procedures; and (3) address the risk of a data breach or theft by employees.

Austin Office
600 Congress Ave.,
Ste. 2100
Austin, TX 78701
512 495-6000 o
512 495-6093 f

Houston Office
711 Louisiana St.,
Ste. 1600
Houston,TX 77002
713 615-8500 o
713 615-8585 f

mcginnislaw.com