RESOURCES

Your Business Has Been Hacked, Now What?

Due to the increasing number of attacks by computer hackers and malicious software (or malware) all businesses should have a plan in place in the event their computer system is compromised. Depending on the nature of your business and the types of personal information your business maintains with respect to its customers, certain legal obligations may be triggered upon discovery of a hack or breach of your business's computer systems. One of these obligations may include a requirement to notify all potentially affected customers in a short amount of time.

Some breach notification laws only apply to certain types of businesses. For example, most medical practices and healthcare professionals must comply with HIPAA and HITECH federal regulations which require notification to patients when patients protected health information may have been accessed, including by a hacker or malware. Further, if you business is a financial institution you may have to comply with the Gramm Leach Bliley Act and other federal and state regulations.

However, all businesses in North Carolina should be aware of the North Carolina Identity Theft Protection Act ("NCITPA") and ensure compliance with the Act in the event of a hack or breach. The NCITPA applies to any business that owns or licenses personal information of residents of North Carolina or any business that conducts business in North Carolina that owns or licenses personal information in any form, whether computerized, paper or otherwise. The personal information protected by the NCITPA includes customer's social security or employer tax identification numbers, driver's license numbers, identification card or password numbers, checking account numbers, savings account numbers, credit card numbers, debit card numbers, PIN codes, electronic identification numbers, digital signatures, biometric data, fingerprints, passwords, a parent's sir name prior to marriage and any other numbers or information that can be used to access a person's financial resources.

If a business is hacked and its computer system containing this protected information is subject to a security breach, then the business may have to provide notice to all affected costumers without unreasonable delay and to the North Carolina Attorney General. A security breach occurs when there is unauthorized access to and acquisition of unencrypted and unredacted records or data containing protected personal information where illegal use of the information has occurred or is reasonably likely to occur or that creates a material risk of harm to a customer. Thus, if a business maintains this protected information regarding its customers it may be subject to the Act and upon discovery of a hack or security breach of its computer systems may have to notify all of the affected customers. Depending on the number of consumers affected, this can be a very costly and a time consuming process.

Additionally, forty six other states currently have similar breach notification laws requiring notification to customers whose information may have been compromised. Businesses in North Carolina who have been hacked or had a security breach should also consult the breach notification laws in other states, especially if they do business in those states and maintain personal information about residents of other states.

Businesses should be prepared for a security breach by having a plan in place. The plan should include securing all protected personal information of customers by hiring forensic IT specialists to investigate and remediate the breach, contact law enforcement, begin the notification process, prepare applicable media and other notifications, and be prepared to respond to customer inquiries. Additionally, businesses can further protect themselves by obtaining insurance policies for such an event. However, beware that general commercial liability insurance policies may exclude cyber liability risks including the cost to comply with breach notification laws. Thus, businesses may want to obtain a specific cyber liability insurance policy if your business maintains customers'

protected personal information.

Carruthers & Roth, P.A.
(336) 379-8651
235 North Edgeworth Street
P.O. Box 540 (27402)
Greensboro, NC 27401