CYBERSECURITY: THREATS, SOLUTIONS AND PROTECTION

Robert N. Young, Director
Carruthers & Roth, P.A.
Email: rny@crlaw.com
Phone: (336) 478-1131

CARRUTHERS & ROTH, PA
ATTORNEYS AT LAW

TOPICS

1. Threats to your business's data
2. Legal obligations and duties to your customers
3. Potential liability
4. Ways to protect your business

CARRUTHERS & ROTH, PA
ATTORNEYS AT LAW

COMMON THREATS TO YOUR BUSINESS'S DATA

I. Cyber Threats
   1. Email
   2. Internet/websites

II. Stolen or lost devices containing data

CARRUTHERS & ROTH, PA
ATTORNEYS AT LAW

CYBER THREATS

1. Most common phishing and/or social engineering (i.e., package ready for pick up, court appearance, account overdue)
2. Malware and other viruses on websites
   - Zero day vulnerabilities
3. Ransomware (i.e., CryptoLocker)

CARRUTHERS & ROTH, PA
ATTORNEYS AT LAW

LEGAL OBLIGATIONS REGARDING CUSTOMER INFORMATION

1. Generally, Business' s duty depends on its business

   - HIPAA (medical practices and business associates that handle protected health information or PHI)
   - Gramm- Leach-Bliley (financial institutions and **"others who receive nonpublic information from financial institutions"**, i.e. car dealers)
   - FTC Act prohibits "unfair and deceptive trade practices in or affecting commerce"

2. Ethics Rules of Professional Conduct
3. Contractual obligations (i.e., contracts with vendors and other service providers including credit card companies)
4. North Carolina Identity Theft Protection Act

CARRUTHERS & ROTH, PA
ATTORNEYS AT LAW

NORTH CAROLINA IDENTITY THEFT PROTECTION ACT (N.G.G.S. § 75-60 ET SEQ.)

- Effective December 1, 2005
- Generally obligates **all businesses** to protect client's social security numbers and other client personal information
- Credit reporting agencies to place security freezes in certain circumstances
- obligates businesses to destroy records with personal information
- protect customers' information from security breaches and
- notify individuals in the event of a breach

CARRUTHERS & ROTH, PA
ATTORNEYS AT LAW

NORTH CAROLINA IDENTITY THEFT PROTECTION ACT; BROAD DEFINITION OF "BUSINESS"

"A sole proprietorship, partnership, corporation, association or other group however organized and whether or not organized to operate at a profit. The term includes a financial institution organized, chartered or holding a license or authorization certificate under the laws of this state and any other state, the United States or any other country, or the parent or the subsidiary of any such financial institution. Businesses shall not include any government or government or subdivision or agency."

Does not exclude entities subject to HIPAA or GLB

CARRUTHERS & ROTH, PA
ATTORNEYS AT LAW

SOCIAL SECURITY NUMBER PROTECTION

A business may not intentionally:

1. Communicate or otherwise make available to the public an individual's social security number.
2. Intentionally print or imbed an individual's social security number on any card required for the individual to access products or services provided by the person or entity
3. Require an individual to transmit his or her social security number over the internet unless the connection is secure or the social security number is encrypted

CARRUTHERS & ROTH, PA
ATTORNEYS AT LAW

CONTINUED….

A business may not intentionally:

4. Require an individual to use his or her social security number to access an internet website unless a password or unique personal identification number or other authentication device is also required to access the internet website
5. Sell, lease, loan, trade, rent or otherwise intentionally disclose an individual's social security number to a third party **without written consent to the disclosure from the individual** and the party making the disclosure knows or in the exercise of reasonable diligence would have reason to believe that the third party lacks legitimate purpose for obtaining the individual's social security number

CARRUTHERS & ROTH, PA
ATTORNEYS AT LAW

EXCEPTIONS TO SOCIAL SECURITY NUMBER PROTECTION

1. Application for a credit report to a credit reporting agency
2. Internal verification or administrative purposes
3. To open an account or to pay for services authorized by an individual
4. To prevent fraud and research by credit reporting agencies and other financial institutions
5. To a business acting pursuant to a court order, warrant, subpoena or when otherwise required by law
6. To a business providing a social security number to a federal, state or local government entity, including law enforcement
7. When the social security number has been redacted

OTHER PROTECTIONS FOR SOCIAL SECURITY NUMBERS

"A business covered by this section **shall** make reasonable efforts to cooperate, through systems testing or other means, to ensure that the requirements of this Article are implemented."

- Important – this creates a duty for all businesses to safeguard and protect social security numbers and have systems testing to make sure they are in compliance with this section.
- A violation of this section is an unfair and deceptive trade practice which could subject your business to treble damages and an award of attorney's fees

CARRUTHERS & ROTH, PA
ATTORNEYS AT LAW

PROTECTED PERSONAL INFORMATION

1. Includes a person's first name and/or first initial and last name in combination with any of the following:
    a. Social security number or employer tax payer identification number
    b. Driver's license, state identification card or passport number
    c. Checking account number
    d. Savings account number
    e. Credit card and debit card number
    f. PIN numbers
    g. Electronic identification numbers, email or address entered in account numbers or internet identification names
    h. Digital signatures
    i. **Any other numbers or information that can be used to access a person's financial resources**
    j. Biometric data
    k. Fingerprints
    l. Passwords
    m. Parent's legal surname prior to marriage
2. If your business maintains any of this information it must take reasonable steps to safeguard this information and if this information is compromised and it is determined a breach of this information has occurred, then notification requirements are triggered.

CARRUTHERS & ROTH, PA
ATTORNEYS AT LAW

BUSINESSES THAT MUST PROTECT CUSTOMER INFORMATION FROM A BREACH

- 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) shall provide notice to the affected person that there has been a security breach following discovery or notification of the breach.
- If business does not own data, but maintains the data, the business must notify the owner of the data (i.e. vendors)

CARRUTHERS & ROTH, PA
ATTORNEYS AT LAW

WHAT CONSTITUTES A BREACH?

- A security breach is defined as “an incident of unauthorized access to and acquisition of unencrypted and unredacted records or data containing personal information or illegal use of the personal information has occurred or is reasonably likely to occur or that creates a material risk upon to a consumer.”
- Any incident of unauthorized access to and acquisition of encrypted records or data containing personal information, along with the confidential process or key shall constitute a security breach. **(safe harbor-not a breach if data is encrypted)**
- Good faith acquisition of personal information by an employee or agent of the business for a legitimate purpose is not a breach provided that the personal information is not used for an unlawful purpose or subject to further unauthorized disclosure.

AFTER A SUSPECTED BREACH

- If a breach is suspected (i.e., a virus or malware is found on your computer or if a laptop or phone is lost or stolen) then businesses should conduct a risk assessment and determine whether the unauthorized access or acquisition of unencrypted and unredacted records containing protected personal information constitutes a breach.
- If it is determined that a breach has occurred then the business must notify the affected individuals.

NOTIFICATION REQUIREMENTS

1. Specific notification requirements, including a description of the incident, types of personal information that was accessed, a description of the general acts and the business to protect the personal information from further access, a telephone number for the business, advice that directs the persons to remain vigilant and review account statements.
2. The toll free number of the major consumer reporting agencies and the toll free numbers, addresses and websites of the Federal Trade Commission for the North Carolina Attorney General's Office.
3. Typically this is done by written notice but can be done with electronic or telephone notice under limited circumstances. If the cost of notification is over $250,000 or the number of persons affected is over 500,000, a business may offer substitute notice, including posting on their website and notice to major statewide media.

NOTIFICATION REQUIREMENTS CONTINUED…

4. If a business notifies individuals it must also notify the Consumer Protection Division of the North Carolina Attorney General's Office. If the breach affects over more than 1,000 people it must notify all consumer reporting agencies.
5. Businesses cannot have customers waive these obligations and businesses subject to the Gramm-Leach–Bliley Act or financial institutions are exempt from this section.
6. This Act does create a private right of action for a consumer who is injured as a result of a breach and is a violation of North Carolina Unfair and Deceptive Trade Practices.
7. The North Carolina Act only applies to information of North Carolina residents. **If your business has clients that reside in other states then you must consult those state statutes for their notification requirements.**
8. Currently 47 states have breach notification laws with varying degrees of severity. Note, some states have specific safeguarding requirements but not North Carolina.

C|R
CARRUTHERS & ROTH, PA
ATTORNEYS AT LAW

NOTIFICATION TO CUSTOMERS

1. The notification must be made without unreasonable delay and it must be consistent with the legitimate needs of law enforcement and the business must restore their reasonable integrity security and confidentiality of the data system.
2. There is a safe harbor provision to delay notification if a law enforcement agency informs the business that the notification may impede a criminal investigation.

CARRUTHERS & ROTH, PA
ATTORNEYS AT LAW

OBLIGATIONS REGARDING THE DESTRUCTION OF RECORDS THAT CONTAIN PERSONAL INFORMATION

Any business that conducts business in North Carolina and maintains personal information of a resident of North Carolina must take reasonable measures to protect against unauthorized access to or use of the information in connection with or after its disposal.

CARRUTHERS & ROTH, PA
ATTORNEYS AT LAW

PROTECTING DATA DURING DISPOSAL

Reasonable measures for the protection of personal information during disposal include:

1. Implementing and monitoring compliance with policies and procedures that require the destruction of papers containing personal information and the erasure of electronic media.
2. Businesses must have written policies relating to the adequate destruction or proper disposal of records containing personal information.
3. This obligation can be met if a business enters into a written contract with a third party engaged in the business of record destruction. Note, this section does not apply to financial institutions or healthcare facilities subject to HIPAA or consumer reporting agencies, however, these entities are also subject to federal regulations which require the safeguarding and destruction of personal information.
4. Individuals may bring a private right of action for violations of this section if they are injured under the North Carolina Unfair and Deceptive Trade Practices Act. Damages are only trebled if the business was negligent in the training, supervision or monitoring of their employees.

POTENTIAL LIABILITY FOR FAILURE TO COMPLY WITH THE APPLICABLE STATUTES

1. Claims by customers for actual damages suffered (i.e., breach of fiduciary duty, breach of contract, negligence).
2. Regulatory investigations and fines (i.e., the North Carolina Attorney General, OCR, and the FTC) –FTC v. Wyndham
3. Loss of goodwill and business reputation.
4. Loss of customers

CARRUTHERS & ROTH, PA
ATTORNEYS AT LAW

WAYS TO PROTECT YOUR BUSINESS FROM LIABILITY

1. Computer hygiene
    a. Keep up to date anti virus and anti malware software on all computers
    b. Require complex passwords and regularly change passwords
    c. Do not download or update a program unless you are specifically looking for it (if you want an update go to the actual website, i.e., flash updates)
    d. Do not open any link with an .exe suffix or some unusual suffice without consulting with your IT department
    e. Do not visit unknown websites unless they are work related and you have a high degree of confidence in the website

CARRUTHERS & ROTH, PA
ATTORNEYS AT LAW

WAYS TO PROTECT YOUR BUSINESS FROM LIABILITY CONTINUED…

2. Have the proper employee policies and training in place regarding the protection of personal information
   a. Policies regarding the safe destruction of records and data containing personal information and protection of social security numbers (**statutory requirements**)
   b. Have a breach response plan in place
   c. Have the ability to make sure all laptops, phones and any other portable electronic devices that contain personal information have proper passwords and/or are encrypted.
   d. Ensure there is a mechanism to erase data remotely from portable electronic devices that contain customers' personal information

CYBER LIABILITY INSURANCE POLICIES

Clients are starting to request Certificates of Insurance (COI) with respect to cyber liability policies.

QUESTIONS?

Robert N. Young
Carruthers & Roth, P.A.
Email: rny@crlaw.com
Phone: (336) 478-1131

CARRUTHERS & ROTH, PA
ATTORNEYS AT LAW