SMALL BUSINESS ID THEFT AND FRAUD

PRIVACY AND SECURITY LAW BEST PRACTICES GUIDE FOR SMALL BUSINESS

"NON-COMPLIANCE OF PRIVACY AND SECURITY LAWS COULD INCLUDE LAWSUITS, FINES, AND PENALTIES AND COULD NEGATIVELY AFFECT YOUR BUSINESS"
Michael Benoit – Partner, Hudson Cook LLP

eBook sponsored by:
MERCHANTS INFORMATION SOLUTIONS
ID THEFT ADVISORY BOARD

Small Business Information Security and Governance Best Practices Guide

TABLE OF CONTENTS

Privacy & Security Law Compliance and your Small Business

Small business compliance and regulatory drivers include privacy and security laws and as a result, are now a focal point for many small business owners.

Specifically, small businesses that use, store, transfer, and/or own Personally Identifiable (non-public) Information (PII) such as employee or customer data including but not limited to a credit card number, checking account number, social security number, driver's license number, or professional license number must implement reasonable security procedures to protect an individual's PII.

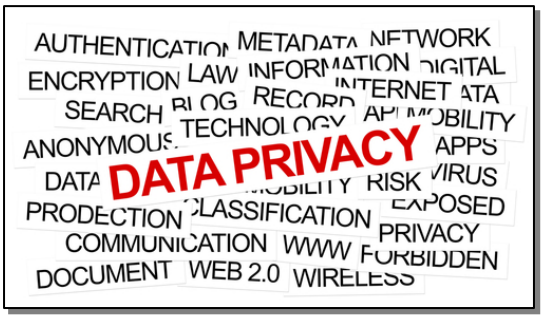
Since 2004 – when California enacted the first state breach notification law in the United States – many other federal and state legislative and regulatory agencies have enacted similar notification laws.

And what was once considered a big business regulatory requirement and responsibility, these privacy and security laws now cover almost every business (large and small) in almost every industry group or business sector in almost every state.

The initial foundation for privacy and security laws was based on how personal information can be used to initiate fraudulent activities that appear to be in the name of an individual consumer for financial gain.

However, more recent privacy and security laws now include protections for individuals whose PII is related to non-financial, fraudulent events such as driver's license information.

As a small business owner, it is important to be aware of a number of **federal and state privacy and security laws** that can apply to small businesses including but not limited to the following:



eBook

FTC Red Flags Rule is a U.S. federal law that requires certain businesses that fall under the FTC's definition of a "creditor" that has "covered accounts" to have an ID theft "prevention, detection and mitigation" plan in place if the breach of customer information could lead to potential ID theft event(s). Enforcement of the new Red Flags rule has now been in effect since December 31, 2010.

Red Flags Rule Checklist:

- Identify Covered Accounts
- Identify Red Flags
- Develop internal procedures to detect Red Flags
- Determine appropriate responses to detected Red Flags
- Implement Identity Theft Prevention Program training
- Identify and review Service Provider agreements for compliance Theft Prevention Program
- Develop a Red Flags Rule Protocol
- Plan for an annual Red Flag review

Health Information Portability and Accountability Act (HIPAA) is a U.S. federal law that has evolved in security law – also known as the **Health Information Technology for Economic and Clinical Health Act (HITECH Act)** that requires a data breach notification for business associates. Business associates are companies like accounting firms, billing agencies, law firms and/or other businesses that provide services to entities like hospitals, medical groups, dental groups, pharmacies, and other healthcare related companies. With the change in the HITECH privacy provisions related to ARRA (American Recovery and Reinvestment Act of 2009), the business associate now has responsibility and liability directly for a breach. This new HITECH provision has been effective since February 17, 2010.

HIPAA HITECH Checklist:

- Identify the individual with responsibility for privacy security
- Create a written privacy security policy

- Implement an annual privacy security policy assessment
- Update privacy policy every annually
- Provide regularly scheduled privacy security training to all employees

A third regulatory and compliance driver for small businesses are the current **46 state Security Breach Notification Laws,** along with the District of Columbia, Guam, Puerto Rico, and the Virgin Islands. In each instance, each state breach notification law requires your business – regardless of size – to notify any employee, customer and/or member of a data breach event where employee, customer and/or member PII may have been lost or stolen.

State Security Breach Notification Law Checklist:

- Annual confirmation of the states your customers and employees are located in
- Current review of state breach notification laws where your business conducts business
- Understanding of personal information that is subject to the breach notification law(s) where your business conduct business
- Understanding the state breach notification process ranging from securing data to contacting law enforcement to notifying the state attorney general's office (or designated regulated agency) to notifying affected employees and/or customers

Children's Online Privacy Protection Act (**COPPA**) is a U.S. federal law created to protect children's privacy and safety online including restrictions on the marketing to those under 13. The act, effective April 21, 2000, applies to the online collection of personal information by persons or entities under U.S. jurisdiction from children under 13 years of age. It details what a website operator must include in a privacy policy, when and how to seek verifiable consent from a parent or guardian, and what responsibilities your business has as an operator.

COPPA Checklist:

- Post a privacy policy on the homepage of the website operator and link to the privacy policy everywhere personal information is collected
- Provide notice to parents about the site's information collection practices

- Give parents the choice to consent to the collection and use of a child's personal information and for said information to not be disclosed to third parties
- Provide parents with access to their child's information, and the opportunity to delete the information and opt out of the future collection or use of the information
- To not require a child's participation in an activity on the disclosure of more personal information than is reasonably necessary for the activity
- Maintain the confidentiality, security and integrity of the personal information collected from children

Payment Card Industry Data Security Standard (PCI DSS) is an information security standard for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and POS cards. Defined by the Payment Card Industry Security Standards Council, the standard was created to increase controls around cardholder data to reduce credit card fraud via its exposure. Validation of compliance is done annually — by an external Qualified Security Assessor (QSA) for organizations handling large volumes of transactions, or by Self-Assessment Questionnaire (SAQ) for small businesses handling smaller volumes.

PCI DSS Checklist:

- Install a firewall to protect cardholder data
- Do not use vendor-supplied defaults for system passwords
- Protect stored cardholder data
- Encrypt transmission of cardholder data
- Use and regularly update anti-virus software
- Restrict access to cardholder data by business need to know
- Assign a unique ID to each person with computer access
- Restrict physical access to cardholder data
- Regularly test security systems and processes
- Maintain a policy that addresses information security for all personnel

Based on the above privacy and security laws, small business owners need to understand how their business relates to each law and how their business needs to respond in the event of a data breach event.

According to the Privacy Rights Clearinghouse (PRC), which is a San Diego, California based, nonprofit consumer organization that tracks and reports on privacy and security laws along with publicly known data breach events, there are eight (8) types of Data Breaches including:

- Unintended disclosure (DISC**)** - Sensitive information posted publicly on a website, mishandled or sent to the wrong party via email, fax or mail.
- Hacking or malware (HACK) - Electronic entry by an outside party, malware and spyware.
- Payment Card Fraud (CARD) - Fraud involving debit and credit cards that is not accomplished via hacking. For example, skimming devices at point-of-service terminals.
- Insider (INSD) - Someone with legitimate access intentionally breaches information - such as an employee or contractor.
- Physical loss (PHYS) - Lost, discarded or stolen non-electronic records, such as paper documents.
- Portable device (PORT) - Lost, discarded or stolen laptop, PDA, smartphone, portable memory device, CD, hard drive, data tape, etc.
- Stationary device (STAT) - Lost, discarded or stolen stationary electronic device such as a computer or server not designed for mobility.
- Unknown or other (UNKN)

A small business owner needs to be aware of and clearly understand the types of data breach events that can impact their small business.

A 5 step checklist to privacy and security compliance should include the following elements:

- Understanding how a data breach can negatively impact your small business revenue, profits and brand reputation

- Complete awareness and understanding of federal and state privacy and security laws
- The creation of a data breach incident plan to respond to federal and state security laws
- Establishment of and regularly scheduled risk assessments ranging from the type of information your small business uses/owns to how your small business safeguards said information
- Education and training for all employees – whether your small business has one employee or 10 employees – on the privacy and security laws and information governance and security

NOTICE AND DISCLOSURE

This eBook is not intended to offer professional consulting services or legal advice. This eBook is intended to provide basic direction, guidance and concepts for small business owners and small business executives.

No one company can ever prevent itself from having an ID Theft, data breach or fraud event. Merchants Information Solutions, Inc. (Merchants) and its Advisory Board recommends all companies and organizations seek professional consulting services and legal advice regarding the content of this document.

This eBook is a working document and will be updated to reflect Small Business ID Theft and Fraud trends and regulatory/compliance updates on an ongoing basis.

Contributing Authors:

Michael Benoit
Partner
Hudson Cook, LLP
http://www.hudsoncook.com/

David G. Beauchamp
Partner
Bryan Cave, LLP
http://www.bryancave.com/offices/phoenix/

Mark Pribish
VP & ID Theft Practice Leader
Merchants Information Solutions, Inc.
www.merchantsinfo.com