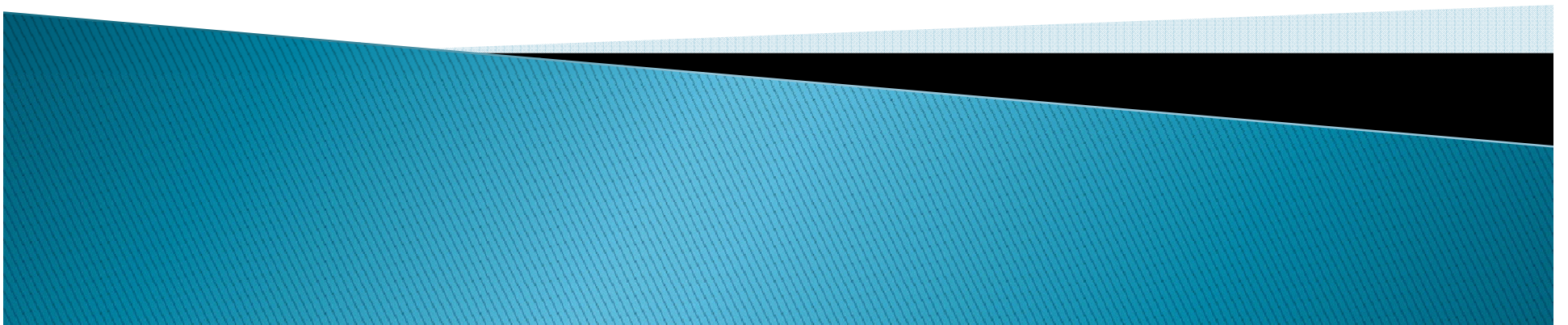


201 CMR 17.00

Identity Theft & Fraud Protection for
Massachusetts Residents



It's NOW available!

- ☑ The Essential Guide for
201 CMR 17.00 Compliance
- ☑ Risk-Based Analysis template
- ☑ The Your WISP template and
- ☑ Accompanying materials

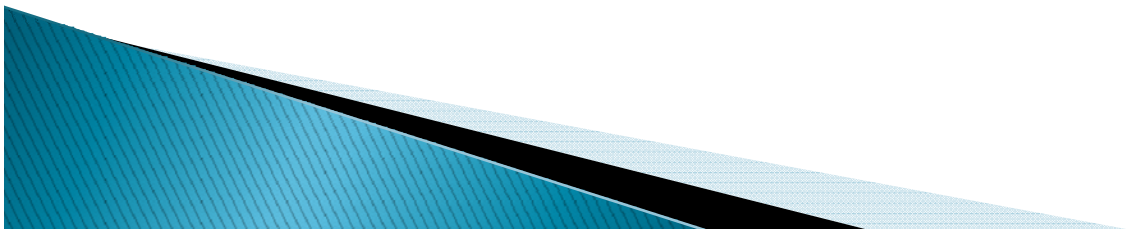
Copyright Notice

- ▶ © November 2009 Joe Burns
 - All rights reserved
- ▶ This PowerPoint presentation is a part of The Essential Guide for 201 CMR 17.00 Compliance, which includes the Guidebook, the Your WISP template, Risk-Based Analysis template and accompanying materials, published by iComplyNow, a unit of ITLNOW, Inc.
- ▶ No part of this presentation may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or any information storage and retrieval system, without written permission from the publisher, except for the inclusion of brief quotation in a review

What is 201 CMR 17.00?

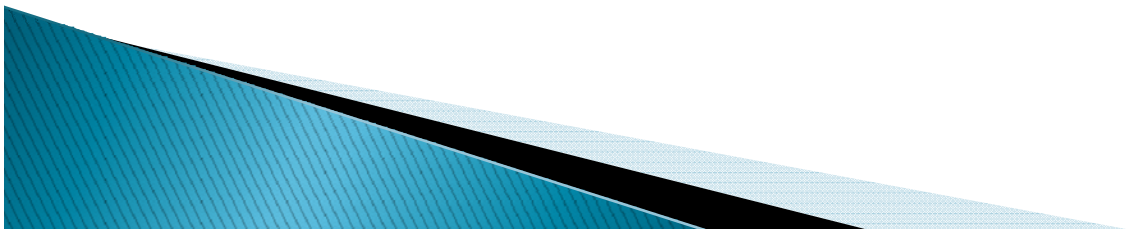
- ▶ Implements the provisions of MGL c. 93H for:
 - safeguarding Personal Information (PI) in both paper and electronic records
 - insuring the security and confidentiality of customer information in a manner fully consistent with industry standards:
 - protects against anticipated threats or hazards to the security and integrity of such information
 - protects against unauthorized access to or unauthorized use of such information that may result in substantial harm or inconvenience

- ▶ Effective March 1, 2010



Who Must Develop a WISP

- ▶ Every person who owns or licenses personal information must develop, implement and maintain a comprehensive Written Information Security Program (WISP):
 - written in one or more readily accessible parts
 - contains administrative, technical and physical safeguards appropriate to:
 - the size, scope and type of business
 - the amount of resources available to the business
 - the amount of stored data (PI)
 - the need for security and confidentiality of both consumer and employee information



What is Personal Information (PI)

- ▶ (First Name + Last Name) or (First Initial + Last Name) in combination with one or more of the following:
 - social security number
 - driver's license or state-issued identification card
 - financial account number or credit or debit card number with or without any required security code, access code, personal identification number or password
- ▶ Personal information relative to residents of the Commonwealth of Massachusetts, ONLY
- ▶ Does not include personal information lawfully obtained from publicly available information or from federal, state or local government records lawfully made available to the public

201 CMR17 Compliance Checklist

STEP	201CMR17	Regulatory Requirement
1	Section 17.03: (2) (a)	designating one or more employees to maintain your WISP
2	Section 17.03: (2) (b)	performing an internal and external risk assessment of your current information security program's procedures for safeguarding personal information stored in paper and electronic form, and evaluating and implementing improvements for securing personal information
3	Section 17.03: (2) (c)	developing or amending security policies for storage, access and transportation of records containing PI outside of business premises
4	Section 17.03: (2) (d)	imposing disciplinary measures for violations your WISP's rules
5	Section 17.03: (2) (e)	preventing terminated employees from accessing PI
6	Section 17.03: (2) (f)	overseeing third-party providers contract(s) for maintaining appropriate security measure for PI consistent with the regulations
7	Section 17.03: (2) (g)	restricting physical access to records containing PI and storage of such PI in locked facilities
8	Section 17.03: (2) (h)	monitoring your WISP to insure that is operating as planned to safeguard your PI
9	Section 17.03: (2) (i)	reviewing the scope of security measures, at least, annually or whenever there has been a material change in your business practices that reasonably impact the security or integrity of records containing PI and making adjustments to your WISP as necessary
10	Section 17.03: (2) (j)	documenting responsive actions taken in connection with any incident involving breach of security

201 CMR17 Compliance Checklist

STEP	201CMR17	Regulatory Requirement
1	Section 17.04: (1)	implementing secure user authentication protocols
2	Section 17.04: (2)	implementing secure user access control measures
3	Section 17.04: (3)	encrypting transmitted records and files containing PI across public networks or wirelessly
4	Section 17.04: (4)	reasonable monitoring of systems for unauthorized use or access to PI
5	Section 17.04: (5)	encrypting all PI stored on laptops or other portable devices
6	Section 17.04: (6)	reasonably up-to-date firewall protection and operating system security patches for maintaining the integrity PI
7	Section 17.04: (7)	reasonably up-to-date version of system security agent software which must include malware an virus protection and set to receive security updates on a regular basis
8	Section 17.04: (8)	educating and training employees in the proper use of the computer security system and the importance of PI security

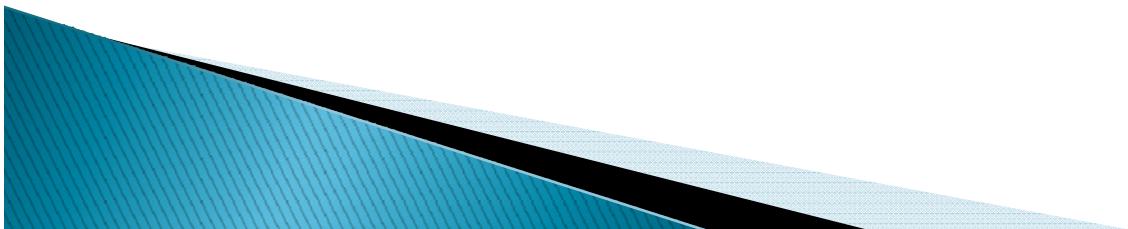
Are You Ready to Comply?

How Ready is Your Company for 201CMR17 Compliance?	Your Situation
Number of employees (that contain personal information)	
Number of customers, clients, or accounts that contain personal information (PI)?	
Do you use 3 rd -party service providers who have access to or use of your PI?(how many)	
Do you have in house IT resources? (yes, no, somewhat)	
Do you have in house HR resources? (yes, no, somewhat)	
Do you have a policy and procedures manual for employees? (yes, no, somewhat)	
Do you have employee job descriptions? (yes, no, somewhat)	
Do you have a written information security program (ISP)? (yes, no , somewhat)	
If you have an ISP, is it 201CMR17 compliant? (yes, no, somewhat)	
Do you have on board expertise in writing security policies and procedures? (yes, no, somewhat)	
Do you have on board expertise for implementing the technologies required to comply with 201CMR17? (yes, no, somewhat)	



Importance of Policies & Procedures

- ▶ Only one (1) Section of 201 CMR17 explicitly requires a policy (Section 17.03: (2) (c))
- ▶ However, our “Your WISP” template includes many sample policy(s) and procedure(s) to be used as a business **Best Practice**:
 - **Policies** establish **WHAT** your business intends to do to be compliant
 - **Procedures** set forth **HOW** your business has implemented compliant actions

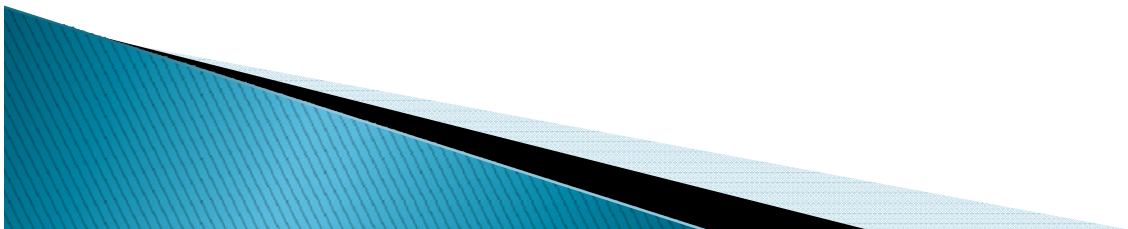


Risk-Based Approach to WISP Development

- ▶ According to the OCABR FAQs: A risk-based approach directs a business to establish a comprehensive WISP that takes into account the particular business':
 - Size
 - Scope of business
 - Amount of resources
 - Nature and quantity of data collected and stored
 - Need for security

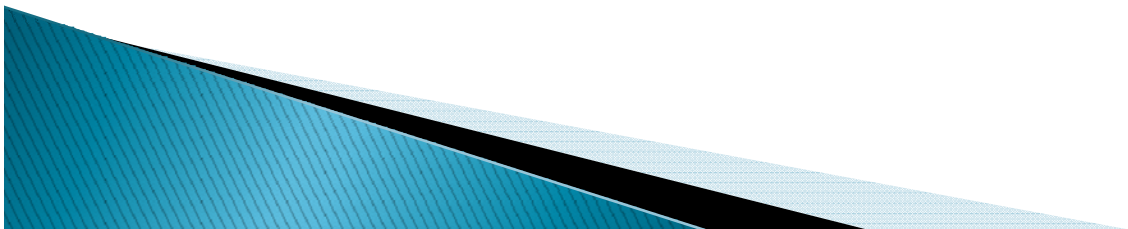
- ▶ NOTE:
 - A risk-based approach is especially important to those small businesses that do not handle or store large amounts of personal information

 - If you are a small business, you need to assess the need for your business to comply with each and every step of the regulations – some regulations may not apply



Enforcement

- ▶ Massachusetts Attorney General – MGL c. 93A (4)
 - Civil penalties of not more than \$5,000 per violation
 - Restraint and injunctive relief
 - Reasonable costs for investigation and litigation, including reasonable attorneys fees
- ▶ Potential civil actions
- ▶ Remember:
 - As of today, you are not required to FILE your WISP with any government agency BUT like most government regulations, ignoring the requirements of 201CMR17 is not acceptable compliance

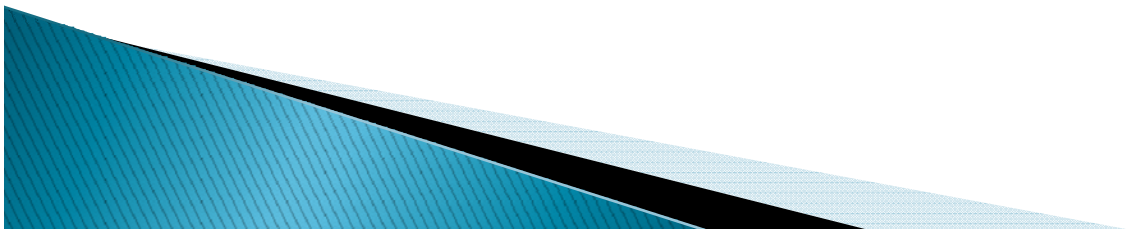


What Most Would Like you to Think

- ▶ 201CMR17 represents a target rich opportunity for overcharging the unknowing. Fear, Uncertainty, and Doubt (FUD). It's the way of big consulting:
 - Just enough “techno babble” to confuse most small to medium size business owners
 - Just enough legalese to scare most small to medium size business owners
- ▶ OCABR estimates:
 - 10 person business with 3 laptops, 1 network server and 7 desktop PCs
 - One time cost: \$ 4,000
 - Recurring: 6,000
 - Total: \$ 10,000
 - Word on the street has it that you could reasonably expect to pay between \$15,000 – \$30,000 depending on the particular third-party service provider

Your Choice (the scare tactics)

- ▶ Roll the dice – I’m fine and don’t need anymore government bureaucracy or regulation
- ▶ Bet the ranch – won’t happen to me, I’m bulletproof
- ▶ Risk your hard earned reputation – business loss due to “your” third-party service provider’s violations or breaches
- ▶ **Examples of Bad Behavior:**
 - TJX – 45 million cards stolen, \$9.7 million in penalties, \$256 million to fix “leak(s)” in their computer security system
 - Hannaford Bros – 4.2 million cards stolen, 1800 reported cases of identity theft, unknown amount in penalties, undisclosed amount to fix “leak(s)” in their computer security system, more to come



The TO-DO List!

- ▶ Make a good business decision for your company:
 - Develop a risk-based comprehensive information security program consistent with the regulations and reasonable for your particular circumstances

- ▶ The Essential Guide for 201 CMR17 Compliance:
 - Buy our book: No need to spend a lot of money on consultants, lawyers or other professional “helpers”
 - Do It (most of the work) Yourself (DIY)
 - Modify sample policies, procedures and other documents
 - Follow the reasonable actions for compliance
 - Email us with your issues – we’ll help
 - Sign up for our support agreement – help make the guide better

How do I GET the Guidebook

- ▶ VISIT www.iComplyNow.com and order online
- ▶ For more information email us at info@iComplyNow.com

iComplyNow a unit of ITLNOW, Inc.

31 Home Depot Drive, Suite 136

Plymouth, MA 02360

United States

Sales Telephone: 888-445-4843

Sales Email: sales@iComplyNow.com

Fax: Number: 617-413-1059

Website: www.iComplyNow.com

Technical Fee Based Support Telephone: 888-445-4843

Technical Fee Based Support Email: help@iComplyNow.com

