

Table of Contents

CHAPTER 1. INTRODUCTION

- § 1:1 The problem
- § 1:2 The law—A solution?
- § 1:3 Post-notice risks
- § 1:4 How to get started

CHAPTER 2. GETTING STARTED: DECIDING WHETHER TO NOTIFY

I. DETERMINING WHO REGULATES YOUR ORGANIZATION

- § 2:1 Introduction—What laws apply to you?
- § 2:2 Health care providers
- § 2:3 Health information
- § 2:4 Financial service providers
- § 2:5 Companies that issue mortgages
- § 2:6 Companies that accept credit cards
- § 2:7 Telecommunication companies
- § 2:8 Other miscellaneous industries
- § 2:9 US public companies

II. WAS THERE “TRIGGERING” INFORMATION?

- § 2:10 Introduction—What information was impacted?
- § 2:11 Government identification numbers
- § 2:12 Health care service providers
- § 2:13 Health information
- § 2:14 Financial service providers
- § 2:15 Credit card numbers
- § 2:16 Financial account information
- § 2:17 Other triggering information

III. WAS THAT INFORMATION “COMPROMISED”?

- § 2:18 Introduction—What is a breach, really?
- § 2:19 Unauthorized access or acquisition?

- § 2:20 —Access or acquisition
- § 2:21 —Acquisition and access
- § 2:22 —Health care laws
- § 2:23 —Financial services laws
- § 2:24 —Defining “authorization”
- § 2:25 —Authorization and vendors
- § 2:26 Has there been a compromise of security?
- § 2:27 —Conducting a “risk analysis” under HIPAA
- § 2:28 —Conducting a “risk analysis” under GLB?
- § 2:29 What steps to take when there is “suspicious activity”

IV. DOES AN EXCEPTION APPLY?

- § 2:30 Introduction—Do you fall under an exception?
- § 2:31 Is there really a likelihood of harm?
- § 2:32 Exceptions if required to follow other laws
- § 2:33 —Compliance with primary regulator
- § 2:34 —Compliance with financial regulations
- § 2:35 — —Compliance with GLB generally
- § 2:36 — —Compliance with GLB security standards
- § 2:37 —Compliance with HIPAA
- § 2:38 Exception if have internal policy
- § 2:39 Physical information “exception”
- § 2:40 Exceptions if information encrypted
- § 2:41 Good faith exception

CHAPTER 3. THE HEART OF THE MATTER: CONDUCTING INVESTIGATIONS

I. INTERNAL INVESTIGATION

- § 3:1 Introduction
- § 3:2 Is an investigation required?
- § 3:3 Investigation mechanics
- § 3:4 —How did the breach occur?
- § 3:5 —Was information compromised?
- § 3:6 —What information was impacted?

II. COOPERATING WITH LAW ENFORCEMENT

- § 3:7 Introduction
- § 3:8 Meeting the threshold for delay
- § 3:9 Delay: mandatory or optional?

TABLE OF CONTENTS

- § 3:10 Length of the delay
- § 3:11 Determining whom in law enforcement to contact

III. VENDORS: DUTY TO COOPERATE WITH DATA OWNER

- § 3:12 Introduction
- § 3:13 Defining cooperation

IV. WORKING WITH BREACH VENDORS

- § 3:14 Introduction
- § 3:15 Vendors who can conduct investigations
- § 3:16 Vendors who provide notice services
- § 3:17 Vendors who provide call center services
- § 3:18 Credit monitoring

V. PRIVILEGE

- § 3:19 Maintaining attorney-client privilege
- § 3:20 The engagement letter
- § 3:21 Working with the vendor

CHAPTER 4. WHO IS PAYING FOR THIS?: INSURANCE COVERAGE

- § 4:1 Introduction
- § 4:2 Commercial general liability insurance
- § 4:3 Directors & officers insurance
- § 4:4 Cyber risk insurance

CHAPTER 5. WHEN BREACH LAW IS NOT TRIGGERED: SHOULD YOU NOTIFY ANYWAY?

- § 5:1 Introduction
- § 5:2 Liability risks under deceptive practices laws
- § 5:3 Notifying in countries with “guidelines” (not laws)
- § 5:4 Making the decision

CHAPTER 6. WRAPPING UP: PROVIDING NOTICE

- § 6:1 Introduction

I. NOTICE TO INDIVIDUALS

- § 6:2 In general

- § 6:3 Timing of notice to individuals
- § 6:4 Contents of notice to the individual
- § 6:5 —Online accounts and California residents
- § 6:6 —Massachusetts form notification
- § 6:7 —Prohibited content
- § 6:8 —Use of a universal notice
- § 6:9 Method of notice to individuals
- § 6:10 —Written notification (mail)
- § 6:11 —Email notification
- § 6:12 —Notification by phone
- § 6:13 —Other methods of notification
- § 6:14 —Substitute notice

II. NOTICE TO GOVERNMENT ENTITIES

- § 6:15 Introduction
- § 6:16 Authorities that need notification
- § 6:17 —General breach requirements and government entities
- § 6:18 —Financial service providers and government notice
- § 6:19 —Health care companies government notice
- § 6:20 —Real estate agents and notice to government entities
- § 6:21 —Electronic communications and government notice
- § 6:22 Content of notice to government entities
- § 6:23 Timing of notice to government authorities
- § 6:24 —General notice timing
- § 6:25 —Financial services sector and notice timing
- § 6:26 —Health care entities and notice timing
- § 6:27 Method of notice to government authorities

III. NOTICE TO CREDIT REPORTING AGENCIES

- § 6:28 Introduction
- § 6:29 Content of notice to credit reporting agencies
- § 6:30 Timing of notice to credit reporting agencies

IV. MISCELLANEOUS

- § 6:31 Health care providers and notice to media
- § 6:32 Notification obligations under SEC
- § 6:33 Contractual notice obligations
- § 6:34 —Notice to Fannie Mae and Freddie Mac

TABLE OF CONTENTS

§ 6:35 —PCI and notice requirements

V. VENDORS: NOTIFICATION OBLIGATIONS

- § 6:36 Introduction
- § 6:37 Notification to data owner
- § 6:38 —HIPAA
- § 6:39 Notification directly to individuals
- § 6:40 Timing of notice
- § 6:41 Payment responsibilities

CHAPTER 7. BUT WAIT, THERE'S MORE!: HANDLING POST-NOTICE INQUIRIES

§ 7:1 Introduction

I. HANDLING REGULATOR INQUIRIES

- § 7:2 Introduction
- § 7:3 Data protection requirements
- § 7:4 —Requirements for general industries
- § 7:5 —Requirements for regulated industries
- § 7:6 Preparing for regulator's inquiries
- § 7:7 Inquiries from state regulators
- § 7:8 Inquiries from federal regulators
- § 7:9 Inquiries from international regulators

II. HANDLING CUSTOMER INQUIRIES

- § 7:10 Introduction
- § 7:11 Individual inquiries addressed through PR/Good
FAQs
- § 7:12 Class-action lawsuits

III. HANDLING SHAREHOLDER INQUIRIES

- § 7:13 Introduction
- § 7:14 Examples
- § 7:15 Recommendations

CHAPTER 8. WHAT IF YOU MAKE A MISTAKE? PENALTIES FOR VIOLATING BREACH-NOTICE STATUTES

- § 8:1 Introduction
- § 8:2 Penalties

- § 8:3 Civil causes of action
- § 8:4 HIPAA and GLBA

APPENDICES

Appendix A. U.S. Federal and State Breach Notification
Laws

Appendix B. Non-US Breach Notification Laws

Appendix C. Illustrative Tables

Table of Cases

Index