

EVERYONE'S NIGHTMARE

PRIVACY AND DATA BREACH RISKS



Mark E. Schreiber

Chair, Privacy and Data Protection Group
Boston, MA

+ 617 239 0585

mschreiber@edwardswildman.com

Theodore P. Augustinos

Co-chair, Privacy and Data Protection Group
Hartford, CT

+1 860 541 7710

taugustinos@edwardswildman.com

Laurie A. Kamaiko

Co-chair, Privacy and Data Protection Group
New York, NY

+1 212 912 2768

lkamaiko@edwardswildman.com

The partnerships of Edwards Angell Palmer & Dodge LLP and Wildman, Harrold, Allen & Dixon LLP merged on October 1, 2011. The new firm is Edwards Wildman. Edwards Wildman comprises the following legal entities: Edwards Wildman Palmer LLP, Edwards Wildman Palmer UK LLP, Edwards Wildman Innovations LLP.

This edition is updated as of January 1, 2012. To obtain a copy of this edition by email or to be placed on the mailing list for future editions, please email PrivacyWhitePaper@edwardswildman.com.

EDWARDS
WILDMAN

January 1, 2012

Everyone’s Nightmare: Privacy and Data Breach Risks

TABLE OF CONTENTS

	Page
I. INTRODUCTION	1
1. Personal Information.....	2
2. Breaches of Data Other Than Personal Information	5
a. Secrets of All Sorts	5
b. Cyber Spies	6
c. Cyber Attacks with Physical Effects or Business Disruption as Focus	8
3. The Scope of What Constitutes a “Data Breach”: Not Just Electronic – Paper Too	11
4. Privacy and Data Breach Concerns in Cloud Computing	12
5. Privacy and Data Breach Concerns in Social Media	14
6. Privacy Issues Arising Out of Behavioral Advertising and On-Line Tracking	17
a. In the United States.....	17
(i) The FTC Recommendations	17
(ii) Do Not Track Class Actions	18
(iii) Federal and State Do Not Track Legislation.....	18
b. E.U. Positions on Online Behavioral Advertising	19
c. Canada	19
d. Upcoming	19
7. New Technologies Bring New Risks	20
8. The Breadth of the Problem.....	20
a. The Big Picture: Number of Breaches and Associated Costs	20
b. The Industries, Assets, and Types of Data Most Frequently Compromised.....	21
c. Causes	22
d. Breach Discovery and Response.....	23
9. The Importance of Timely and Proper Notification.....	24
II. THE REGULATORY AND STATUTORY LANDSCAPE: OBLIGATIONS UNDER DATA PRIVACY AND SECURITY LAWS AND REGULATIONS	25
1. State Data Privacy and Security Requirements.....	25

EDWARDS WILDMAN PALMER LLP

a.	Protection of Social Security Numbers	25
b.	Record Disposal Requirements	26
c.	Data Breach Notification Requirements	27
d.	Massachusetts is at the Forefront in Data Privacy and Security Regulation and is Setting a New Standard.....	29
2.	Federal Requirements	33
a.	Gramm-Leach-Bliley Act – Privacy and Safeguard Rules	33
b.	Federal Trade Commission “Red Flags” Rule	34
(i)	Affected “Financial Institutions” and “Creditors”	35
(1)	Covered Accounts.....	36
(ii)	Federal Information Security Management Act of 2002	37
(iii)	Securities and Exchange Commission Guidance and Enforcement.....	37
(1)	SEC Guidance Regarding Public Company Obligations to Disclose Cyber Security Risks and Incidents to Investors.....	37
(2)	New SEC Enforcement of Data Security Requirements.....	38
(iv)	HIPAA Privacy and Security Rules	39
(v)	The HITECH Act and Health Data Breach Notification Rules	40
(1)	FTC Health Breach Notification Rule	40
(2)	The HHS Breach Notification Rule for HIPAA Covered Entities and Business Associates	42
(vi)	Additional Data Privacy Requirements for Educational Institutions	44
(vii)	On the Horizon	45
(1)	Federal Privacy Frameworks	45
(2)	Proposed Federal Privacy, Data Security and Cyber Security Legislation	46
(3)	Initiatives of the Obama Administration	48
3.	Industry Standards: PCI Standards for the Protection of Credit Card Information	51
a.	Incorporation of PCI-DSS into State Law	52
(i)	Minnesota	53
(ii)	Nevada	53
(iii)	Washington	53

EDWARDS WILDMAN PALMER LLP

4.	International	54
a.	Introduction.....	54
b.	The European Union	54
(i)	E.U. Data Protection Directive	54
(ii)	Cookies and other tracking technologies	56
(iii)	The Dilemma of Whistleblower Hotlines	57
c.	Selected Countries' Data Protection Laws	58
(i)	United Kingdom ("UK")	58
(ii)	Germany	59
(iii)	France	60
(iv)	Spain	60
(v)	Sweden.....	61
(vi)	Mexico	61
(vii)	Canada	62
(viii)	India	62
(ix)	China.....	62
III.	THE EXPOSURES PRESENTED BY DATA BREACHES	63
1.	The Potential Costs and Damages of a Breach	63
a.	First-Party Costs	64
b.	Third-Party Claims	64
(i)	Consumer Claims.....	64
(1)	Article III Standing	65
(2)	Cognizable Injuries	66
(3)	Class Certification	69
(ii)	Bank Claims.....	70
(iii)	Other Third-Party Claims	73
2.	Industries Exposed	73
a.	Retailers	74
b.	Hospitality/Food and Beverage.....	75
c.	Universities and Other Educational Institutions	76
d.	Healthcare Providers and Health Insurers.....	78
e.	Financial Institutions.....	81

EDWARDS WILDMAN PALMER LLP

f.	Payment Processors	83
g.	Law Firms	84
h.	Real Estate Agents	85
i.	Employers of All Varieties	86
j.	Utilities	86
k.	Defense Industry/Military Industrial Complex	87
l.	Other Governmental Entities	89
m.	Vendors	89
3.	Insurance Company Exposures	91
a.	Exposure of Companies in the Insurance Industry as Entities Subject to Data Breaches	91
b.	Potential Insurance Coverage for Data Breaches.....	93
(i)	Cyber Risk/Data Breach/Privacy/Network Security Policies	93
(ii)	Property Policies – First-Party	95
(iii)	Fidelity Insurance – Employee Crime	96
(iv)	CGL – Third-Party Claims	96
(1)	Coverage A	97
(2)	Coverage B	98
(3)	Coverage A and B Hurdle.....	101
(v)	Professional Liability/E&O	102
(vi)	D&O	103
(vii)	Kidnap and Ransom/Cyber Extortion.....	104
IV.	MITIGATION OF DATA BREACH EXPOSURES	104
1.	Compliance	105
2.	Instituting Reasonable Security Procedures.....	105
3.	Limiting Access to Protected Information	105
4.	Training/Awareness	106

January 1, 2012

Everyone's Nightmare: Privacy and Data Breach Risks

I. Introduction

In recent years, there has been an increasing number of well-publicized stories of breaches of confidential information. Recent studies of data breaches confirm that data breaches present a costly and significant exposure to companies in all lines of business. While paper sources of information are still subject to inadvertent or malicious disclosures, the growth of electronically collected, transmitted and stored information has resulted in more and larger data breaches. The frequency and severity of data breaches have resulted in a concomitant increase in potential exposures to companies subject both to their own data breaches and to breaches affecting other entities that collect, maintain or disseminate confidential information on their behalf. While confidential information of all kinds is subject to data breach, recent attention and regulation has been directed at breaches involving personal information of individuals, particularly electronically stored personal information.

There is a growing body of law directed at protecting personal information that is often the subject of data breaches and the target of those seeking to engage in identity theft and use such information for fraudulent financial transactions, in the U.S. at both the state and federal levels, and in other countries. As collection and storage of personal information and other confidential information increases, and further laws and regulations are issued, the exposures to companies are also likely to expand.

Discussed below are (i) the growing body of regulations in the U.S. and worldwide, with a concentration on recent U.S. legal and regulatory developments establishing data security requirements and standards, (ii) exposures presented by data breaches, and (iii) the lines of insurance potentially impacted.

The primary focus of this paper is on breaches involving personal information of individuals. We also, however, discuss breaches and cyber attacks involving other categories of confidential information, as well as some of the privacy issues arising out of new technologies and the increasing use of social media.

This paper is published by Edwards Wildman Palmer LLP for the benefit of clients, friends and fellow professionals interested in these issues. The information contained herein is not to be construed as legal advice or opinion. We provide such advice or opinion only after being engaged to do so with respect to particular facts and circumstances. The Firm is not authorized under the U.K. Financial Services and Markets Act 2000 to offer UK investment services to clients. In certain circumstances, as members of the Law Society of England and Wales, we are able to provide these investment services if they are an incidental part of the professional services we have been engaged to provide.

1. Personal Information

Protecting individuals from identity theft has become a significant focus of U.S. state and federal agencies, and of new state and federal laws and regulations.¹ In the pursuit of this goal, efforts have focused on the security of data concerning consumers, including their personal identification numbers, health information, and financial data such as bank account and credit card information.

In the U.S., these categories of information are generally referred to as “Personal Information.”² Laws and regulations vary from state to state, and between state and federal law, as to exactly what information comprises “Personal Information.” Generally, the definition requires both a name (first initial and last name often suffices), and some additional item of information that could be used to steal a person’s identity or access his or her financial accounts (or, in some cases, healthcare information) without authorization. Thus, with some variations in content and nomenclature, the general definition of Personal Information is as follows:

An individual’s name plus one or more of the following:

- Credit card number;
- Social Security number;
- Driver’s license or government issued identification card;
- Medical insurance identification number; or
- Financial account information;

or, depending on the law or regulation triggered:

¹ As defined in the Federal Fair and Accurate Credit Transactions Act of 2003 (“FACTA”), “identify theft” is a fraud committed using the identifying information of another person. 15 U.S.C. 1681a(q)(3).

² For purposes of this paper, we refer generally to protected information about an individual as “Personal Information.” We note that “personal information” is the term used in the Massachusetts Data Security Regulations, while other statutes use terms such as “personal identifiable information” or “private information.” There are differences in the terminology used in statutes and regulations of various jurisdictions, however, such as “personal information” versus “private information” versus “personally identifiable information” or “PII.” New York General Business Law § 899-aa, for example, defines “personal information” as “information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such natural person,” and defines “private information” as “personal information consisting of any information in combination with any one or more of the following data elements, when either the personal information or the data elements is not encrypted, or encrypted with an encryption key that has also been acquired: (1) Social Security number; (2) driver’s license number or non-driver identification card number; or (3) account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual’s financial account; ‘private information’ does not include publicly available information which is lawfully made available to the general public from federal, state or local government records.” See also New York State Technology Law §208, applicable to State entities as defined by the statute and the New York City Administrative Code, Title 10, §10-501, applicable to City agencies refers to “personal identifying information” that includes a person’s date of birth, mother’s maiden name, and other information not included in New York Gen. Bus. Law §899-aa. Breach notification requirements are generally triggered by unauthorized access to or acquisition of “private information,” but acquisition of “personal information” that is limited to a name or personal mark unaccompanied by other information such as a Social Security number, driver’s license or credit/debit card number may not trigger notification requirements under data protection statutes and regulations. Other states’ statutes refer to “personally identifiable information” (PII), e.g., Wisconsin Statutes 19.68.

EDWARDS WILDMAN PALMER LLP

Other government identification information that could be used for identity theft; or
Password and customer identification numbers that allow access to a financial account without a name.

As regulations directed at protecting Personal Information proliferate, however, the scope of protected information is expanding. The federal Red Flags Rule, discussed below, uses the term “identifying information” to mean any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including any:

- (1) Name, Social Security number, date of birth, official state or government issued driver’s license or identification number, alien registration number, government passport number, employer or taxpayer identification number;
- (2) Unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;
- (3) Unique electronic identification number, address or routing code; or
- (4) Telecommunications identifying information or access device.³

The HIPAA Privacy Rule, also discussed below, protects “individually identifiable health information,” which includes all health information in oral, written, or electronic form that can be identified to a specific individual. Any health information, including demographic information that relates to the past, present, or future physical or mental health or condition of an individual, and with respect to which there is a reasonable basis to believe the information can be used to identify the individual, is protected information under HIPAA.⁴

What constitutes Personal Information subject to legal protection is evolving, with courts interpreting existing statutes more expansively and legislatures considering new statutes. In a February 2011 decision, for example, the California Supreme Court held that the practice of recording customer ZIP Code along with customer names violates a California statute, the Song-Beverly Credit Card Act,⁵ which forbids businesses from requesting “personal identification

³ Telecommunications identifying information and access device are defined in 18 U.S.C. 1029(e). Telecommunications identifying information means the electronic serial number or any other number or signal that identifies a specific telecommunications instrument or account, or a specific communication transmitted from a telecommunications instrument. Access device means any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier, or other means of account access that can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds (other than a transfer originated solely by paper instrument).

⁴ 45 C.F.R. § 160.103.

⁵ Ca. Civ. Code § 1747.08(b).

information” during a credit card transaction that is recorded.⁶ The California Supreme Court noted that the statute demonstrated legislative intent to prohibit retailers from requesting and recording information about cardholders that are unnecessary to the credit card transaction. The Court held that the word “address” in the statutory definition of personal identification information should be construed to encompass not only a complete address, but also the components of an address. The Court expressed concern that unless components of an address were also protected, a retailer could circumvent the statute by collecting almost all the components of an address but simply leaving out one aspect (such as the house number). Companies violating the statute are subject to significant fines. A significant factor in the Court’s decision was the ability of retailers to utilize a software program that could identify the full address of a customer from the name and ZIP Code and use it for marketing purposes for itself or to sell to others. As discussed below, new federal statutes are also under consideration which may impact the scope of what is considered Personal Information.

The increase in concern about protecting individuals’ information that can be used for identity theft has led to what is likely to be a growing practice by companies to report unauthorized access to information that may not itself be protected Personal Information, but can be used to gain access to such Personal Information. Thus, for example, on April 1, 2011, Epsilon Data Management LLC⁷ announced that the customer data of many of its more than 2,500 corporate clients was exposed by an unauthorized entry into Epsilon’s email system. The intruder apparently obtained email addresses and/or customer names. Although email addresses are not generally considered to be Personal Information under U.S. laws and regulations that triggers notification requirements, Epsilon notified its clients, many of whom sent notifications to their customers regarding the unauthorized entry to Epsilon’s database. A major concern was that the hackers could use the email addresses in phishing attacks by sending emails that seemed to come from trusted sources, leading unsuspecting customers to reveal Personal Information that would then be used for identity theft.⁸

A data breach involving unauthorized access to Personal Information triggering notification obligations can result from an event as simple as a loss of a laptop that contains personal information of customers or employees.⁹ In recent years, publicity has focused on large data

⁶ *Pineda v. Williams Sonoma Stores, Inc.*, 2011 WL 446921 (Cal.) (2011); also available at <http://www.courtinfo.ca.gov/opinions/documents/S178241.PDF>. See also *Edwards Wildman Palmer Client Advisory, California Supreme Court’s ZIP Code Decision Exposes Retailers to New Litigation Hazard, Statutory Fines*, April 2011, at http://www.edwardswildman.com/files/upload/CA_Sup_Ct_ZIP.pdf.

⁷ Epsilon provides consulting, marketing data, technology and agency services to major retailers. Elinor Mills, *Who is Epsilon and Why Does It Have My Data?*, news.CNET.com, April 6, 2011.

⁸ “Phishing” is the practice of sending an email that is purportedly from a well-known organization to induce the recipient to reveal information for use in identity theft. The recipient is often lured to a website that appears to belong to a legitimate organization, but that silently redirects the user to a website that then requests and collects the user’s personal information for fraudulent purposes.

⁹ 329 organizations reported 86,455 laptops lost at an average cost of \$6.4 million per company, and overall cost of over \$1 billion. Ponemon, “The Billion Dollar Lost Laptop Problem,” Sept. 30, 2010.

breaches that involve sophisticated attacks by wide-ranging criminal rings on the databases of companies storing Personal Information of thousands or even millions of individuals. Cyber criminals often target institutions that maintain Personal Information of large numbers of individuals in an effort to achieve large returns from their efforts. Publicized data breaches of payment processing companies and retailers in which the credit and debit card information of millions of consumers was obtained by cyber criminals demonstrate the scope of such attacks, and the resultant costs to the targeted company. Costs to victimized companies include the direct costs of assessing and responding to the breach, as well as exposure to third-party claims brought by consumers, employees, and others affected by the breach, and the loss of business from the publicity following a large breach.¹⁰

Not all data breaches involving Personal Information actually result in identity theft. As discussed below, however, the mere occurrence of a data breach involving Personal Information can trigger time-sensitive and broad-ranging notification requirements imposed on the entity that sustained the breach. If the loss or theft of Personal Information does not actually result in identity theft, the company sustaining the breach may be able to avoid or at least minimize common law claims for damages from the individuals whose Personal Information was improperly accessed, but in any event it must comply with applicable statutory and regulatory obligations related to the breach.

2. Breaches of Data Other Than Personal Information

This paper focuses largely on data breaches involving Personal Information, but a data breach can also involve other confidential information, the access to and dissemination of which may cause substantial damages and give rise to legal liability, or can be conducted with the goal of disrupting operations rather than accessing information. Such breaches are discussed below, as the potential exposures they present are significant, and they are generating increasing attention from both those seeking to effect such breaches and those seeking to protect against them.

a. Secrets of All Sorts

Data required to be kept confidential is not limited to Personal Information. Confidential data includes trade secrets, intellectual property, proprietary information (*e.g.*, ideas, techniques, plans, processes, financial data, and similar business secrets) and other confidential information

¹⁰ The typical data breach involves either the inadvertent loss or the criminal theft of data containing Personal Information. However, there is also a theory of data breach referred to as a “voluntary data breach” in which intentional dissemination of information unintentionally results in unauthorized distribution of personal information. In late 2009 Netflix, Inc. was sued based on a claim of “voluntary privacy breach” based on the video rental company’s purported dissemination to contest participants of data sets containing the rental preferences and ratings of subscribers. Although Netflix encrypted the identities of its subscribers in the data sets, the complaint alleges that researchers were able to crack the encryption and identify individual subscribers. The complaint, in the United States District Court for the Northern District of California, pled violations of the Video Privacy Protection Act, which prohibits the disclosure of information identifying a person as having requested or obtained a specific video rental. The parties to the lawsuit reached a confidential settlement in March 2010.

that owners and keepers of such information want to keep secret, and that others may seek to obtain for their own benefit or to harm others.

Significantly, recent studies report that confidential business information is increasingly being targeted by hackers, in recognition that trade secrets, company information about upcoming projects and bids, and similar “corporate intellectual capital” can be a source of financial gain and competitive advantage through unauthorized use or sale to others.¹¹

Data breaches involving confidential data that is not within the applicable definitions of Personal Information do not trigger the protection and notification obligations of the large body of state and federal laws directed at protecting against identity theft. They can, however, result in business losses to the breached company, as well as in liability claims by third parties against the targeted company if they cause damage to others.

b. Cyber Spies

While malicious cyber attacks often target institutions with Personal Information that cyber criminals seek for use in identity theft and unauthorized financial transactions, financial gain through identity theft is not the only goal, and Personal Information is not the only target of cyber criminals. In fact, proprietary intellectual property is generally considered twice as valuable as day-to-day financial and customer data.¹² As a result, a thriving criminal market has evolved for converting stolen trade secrets into cash, according to security experts and law enforcement officials.¹³

The following reported cyber attacks illustrate the range of potential targets:

The November 2011 attack on Japan’s parliament’s electronic mail system;¹⁴

The May 2011 attack on information systems of Lockheed Martin, the nation’s largest military contractor, that reportedly may be tied to a hacking attack on another vendor in March that had supplied coded security tokens;¹⁵

The April 2011 attacks on Sony Corporation’s online gaming network, which reportedly compromised information of over 100 million customers’ records;¹⁶

¹¹ McAfee and Science Applications International Corporation, *Underground Economies: Intellectual Capital and Sensitive Corporate Data Now the Latest Cybercrime Currency*, March 28, 2011.

¹² Byron Acohido, *Social-media tools used to target corporate secrets*, USA Today, March 31, 2011 (citing both Forrester Research and Simon Hunt, Chief Technology Officer of McAfee’s Endpoint Security Division).

¹³ *Id.*

¹⁴ Dean Wilson, *Japanese parliament is under cyber attack*, The Inquirer, November 2, 2011.

¹⁵ Christopher Drew and John Markoff, *Data Breach at Security Firm Linked to Attack on Lockheed*, The New York Times, May 27, 2011; Advisen FPN, Professional Edition, May 30, 2011.

EDWARDS WILDMAN PALMER LLP

The March 2011 attack on RSA, the security division of EMC Corporation, which reportedly resulted in information being extracted from their systems that related to RSA's SecurID authentication products that are used in the security systems of many other large corporations and government entities;¹⁷

The March 2011 attack on online marketing company Epsilon Data Management LLC, which resulted in unauthorized access to email addresses and names of customers (*i.e.*, not Personal Information under most laws) of up to 111 retailers;¹⁸

The attack, reported in February 2011, on the computer networks of five multinational oil and gas companies, that reportedly originated in China;¹⁹

The December 2010 attacks on a number of businesses including Visa, MasterCard and PayPal, reportedly by supporters of WikiLeaks;²⁰

The May 2010 denial of service attack against Media Temple, the Web host for Adobe, ABC, Sony, NBC, Time, Volkswagen and Starbucks, that shut down the host, interrupting access to the hosted sites;²¹

The January 2010 allegation by Google that it and more than 30 other companies were breached in a cyber attack that Google traced to China and that reportedly resulted in the theft of a password system, as well as the compromise of the email accounts of two human rights activists in China;²²

The revelation in November 2009 that hackers had stolen over 1,000 emails and 2,000 other documents from the Climate Research Unit at East Anglia University in the UK;²³

Reports of penetration of the U.S. electrical grid by "cyber spies" in the Spring of 2009;²⁴ and the reported 360 million attempts to penetrate Defense Department networks in 2008.²⁵

¹⁶ Julianne Pepitone, *Massive attack blows crater in Sony brand*, CNN Money, May 10, 2011.

¹⁷ John Markoff, *SecurID Company Suffers a Breach of Data Security*, The New York Times, March 17, 2011.

¹⁸ *And the hits keep on coming for Epsilon*, Office of Inadequate Security, DataBreaches.net, April 2, 2011.

¹⁹ John Markoff, *Hackers Breach Tech Systems of Oil Companies*, The New York Times, February 10, 2011.

²⁰ Mark Clayton, *Did WikiLeaks bring on cyberwar? Maybe a cyber sit-in*, Christian Science Monitor, December 23, 2010.

²¹ *Web Host Shuttered by Cyber Attack*, www.esecurityplanet.com, May 26, 2010.

²² Ariana Eunjung Cha and Ellen Nakashima, *Google China Cyberattack Part of Vast Espionage Campaign, Experts Say*, The Washington Post, January 14, 2010; John Markoff, *Cyberattack on Google Said to Hit Password System*, The New York Times, April 19, 2010.

²³ Keith Johnson, *Climate Emails Stoke Debate*, The Wall Street Journal, November 23, 2009.

²⁴ Siobhan Gorman, *Electricity Grid in U.S. Penetrated by Spies*, The Wall Street Journal, April 8, 2009.

Cyber attacks such as these are not just directed at Personal Information, but at confidential information. An underground market has reportedly developed for stolen company secrets.²⁶ On November 3, 2011, the Office of the National Counterintelligence Executive (ONCIX) released a report dated October 2011, which including findings that U.S. businesses are prime targets of foreign economic and industrial espionage as other countries seek to build up their domestic industries with stolen technology and intellectual property from more advanced U.S. firms; the report specifically identified China and Russia as “aggressive and capable collectors of sensitive U.S. economic information and technologies, particularly in cyber space.”²⁷ The leading areas of theft are reported to be components of the U.S. economy: information technology, military technology, and clean-energy and medical technology.²⁸ U.S. defense officials report that more than 100 countries have tried to break into U.S. networks.²⁹ Networks of at least 760 companies, research universities, Internet service providers and government agencies were reportedly the target of China-based cyber spies in the last decade.³⁰

The energy industry has been a recent target, with cyber attacks reportedly conducted against private and state-owned oil, energy and petrochemical companies, targeting confidential and proprietary information such as project financing bids and exploration plans for oil and gas field operations; such attacks have been dubbed “Night Dragon” and identified as originating primarily in China.³¹

These attacks can have substantial financial impact on their targets, including the loss to the breached entity of its own information and business disruption, and potential contractual breaches and resulting claims by third parties impacted by such information theft.

c. Cyber Attacks with Physical Effects or Business Disruption as Focus

During the last few years, another type of cyber risk has become increasingly prominent: cyber attacks that are directed not at illicit acquisition of information, but rather attacks that are directed at causing (or at least can result in) significant physical effects or business disruption,, including destruction or disruption of computer control systems, and the industrial systems and equipment on which the operations of industrial entities and public utilities depend. One of the

²⁵ Yochi J. Dreazen and Siobhan Gorman, *U.S. Cyber Infrastructure Vulnerable to Attacks*, The Wall Street Journal, May 6, 2009.

²⁶ Acohido, *Social-media tools used to target corporate secrets*, USA Today, March 31, 2011, *supra*.

²⁷ ONCIX, *Foreign Spies Stealing U.S. Secrets in Cyberspace – Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011*, October 2011.

²⁸ *Id.*

²⁹ Siobhan Gorman and Stephen Fidler, *Cyber Attacks Test Pentagon, Allies and Foes*, The Wall Street Journal, September 25, 2010.

³⁰ Michael Riley and John Walcott, *China-Based Hacking of 760 Companies Shows Cyber Cold War*, Bloomberg, December 14, 2011.

³¹ McAfee, *Global Energy Cyberattacks: “Night Dragon,”* February 10, 2011.

newest trends in cyber attacks has been labeled “advanced persistent threats” (“APTs”), malware designed for theft, espionage or sabotage.³²

As the recently-retired U.S. Deputy Secretary of Defense put it on September 28, 2011:

In a development of extraordinary importance, cyber technologies now exist that are capable of destroying critical networks, causing physical damage, and altering the performance of key systems. In the twenty-first century, bits and bytes are as threatening as bullets and bombs.”³³

Some of the developments supporting that conclusion are:

In August 2011 at the Black Hat computer security conference, two employees of the cyber security firm iSec Partners demonstrated that they could unlock and start a car by sending text messages to the car’s alarm system.³⁴

In 2010, it was revealed that the Stuxnet worm had successfully disrupted the logic control system for the centrifuges that Iran uses to enrich uranium, making about 1,000 of them unusable.³⁵ According to reports, the Iranian control system was not connected to the Internet, so it is believed that the Stuxnet virus was transmitted by a USB stick that an unknowing person plugged into an otherwise secure computer.

In January 2008, the Central Intelligence Agency revealed that hackers have infiltrated utilities outside the U.S. and made extortion demands. They were able to shut off power to several cities (which were not identified).³⁶

In March 2007, the Department of Homeland Security conducted a cyber attack exercise at the Idaho National Laboratory. It hacked into a network controlling a medium-sized power generator, and put the generator out of sync with the power grid. There is video footage of the generator shuddering and filling the room with steam and smoke.³⁷

³² Mark Bowden, *Malware Myopia*, The Los Angeles Times, October 23, 2011.

³³ William J. Lynn III, *The Pentagon’s Cyberstrategy, One Year Later*, Foreign Affairs, September 28, 2011.

³⁴ Jennifer Valentine-DeVries, *Hacking Targets Multiply*, The Wall Street Journal, September 9, 2011.

³⁵ Kim Zetter, *How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History*, WIRED, July 11, 2011; Ian Bremmer and Parag Khanna, *Cyberteeth Bared*, The New York Times, December 22, 2010.

³⁶ Siobhan Gorman, *Electricity Grid in U.S. Penetrated By Spies*, The Wall Street Journal, April 8, 2009.

³⁷ Mike M. Ahlers, *Inside a government computer attack exercise*, CNN, October 17, 2011.

EDWARDS WILDMAN PALMER LLP

The scenario of a possible breach of the Supervisory Control and Data Acquisition System (SCADA) of a public utility highlights what many experts seem to believe is a realistic risk.³⁸

Cyber attacks between nations have become “a staple of modern warfare.”³⁹ In addition to the Stuxnet Worm, which one computer security expert stated could only have been conducted “with nation-state support,”⁴⁰ cyber attacks have been reported between hackers in Pakistan and India and between Japan and China. Russia also reportedly launched cyber attacks against both Estonia and Georgia. Demand is apparently being driven by companies in some countries looking to undercut rivals in other parts of the world, and by scam artists seeking to game stocks and commodities markets.

While it is far easier to disrupt control systems or equipment that are connected to the Internet or cell phone networks, examples such as the disruption of the Iran centrifuges demonstrate that shutdowns can be accomplished even to systems not directly connected.

The potential for cyber attacks, and the resulting physical effects and related business interruption, are of particular concern when they involve companies involved in critical infrastructure, such as companies in the energy sector, including those supplying electrical power. In September 2011, the Department of Homeland Security warned that the collective known as Anonymous has threatened attacks against the industrial controlled software that runs factories, power stations, chemical plants, and water and sewage facilities.⁴¹ President Obama confirmed that the electrical power grid was penetrated in 2009, and that the cyber attackers installed software that could be used to disrupt infrastructure components and potentially disrupt service at some future time.⁴² An audit by the Department of Energy’s Inspector General found that cyber security standards for the grid were not adequate to mitigate or address systems-related risks.⁴³

Cyber attacks with physical effects can have substantial financial impact on their targets, including property damage, business interruption and contractual breaches, as well as general third-party claims should the disruption of the target’s operations in turn affect its customers and

³⁸ Finkle, *Reuters, supra*. Kim Zetter, *Confusion Center: Feds Now Say Hacker Didn’t Destroy Water Pump*, www.wired.com/threatlevel/2011/11/scada-hack-report-wrong, November 25, 2011.

³⁹ Siobhan Gorman and Stephen Fidler, *Cyber Attacks Test Pentagon, Allies and Foes*, *The Wall Street Journal*, September 25, 2010.

⁴⁰ William Maclean, *Iran ‘first victim of cyberwar,’* *The Scotsman*, September 25, 2010.

⁴¹ Shuan Waterman, *Hacker group threatens industrial computer systems*, *The Washington Times*, October 17, 2011.

⁴² *Electricity Grid in U.S. Penetrated By Spies*, *The Wall Street Journal*, *supra* at 39.

⁴³ U.S. Department of Energy Office of Inspector General Office of Audits and Inspections, *Federal Energy Regulatory Commission’s Monitoring of Power Grid Cyber Security*, January 2011; see also Siobhan Gorman, *U. S. Intelligence Report Labels Chinese ‘Most Active’ in Economic Espionage; Russia Also Named*, *The Wall Street Journal*, November 4, 2011.

vendors.⁴⁴ Moreover, cyber attacks on state-owned entities and on critical infrastructures, utilities and services raise new and complex issues involving national security and public policy. As a result, the concern for national security standards for critical infrastructure has recently generated a plethora of proposed federal legislation, as discussed below. Other countries have also been focusing on this increasing risk. Britain, like the U.S., is focusing not only on the threat as it affects military and infrastructure, but also on the effect on ordinary businesses.⁴⁵ Britain also hosted the first global conference on cyber space, in October 2011, which was attended by officials from 60 countries.

3. The Scope of What Constitutes a “Data Breach”: Not Just Electronic – Paper Too

Data breach is often thought of only as a cyber risk: a risk associated with electronic processes used for conducting business through computer networks. Most of the attention in the past few years has been on electronic data breaches, particularly on instances of cyber criminals gaining unauthorized access to electronic data maintained by financial institutions, data processors and retailers, and on reports of lost laptops containing confidential information. Often, stories focus on the increasing technical sophistication of cyber criminals (such as the story about how thieves can use portable technology to scan credit card information from a card still in the unsuspecting victim’s pocket).⁴⁶ However, many data breaches still happen the old-fashioned way, through the improper safeguarding or disposal of paper records. Apparently, “dumpster diving” is still a common way for those seeking Personal Information and other confidential information for illicit use to obtain that information.

Moreover, many data protection laws and regulations directed at protecting Personal Information are not limited to electronic data, but also require protection and proper disposal of paper records containing Personal Information. Most U.S. data breach notification requirements, however, apply to breaches involving data in electronic format, and do not extend to Personal Information contained in paper documents.

Data breaches regularly occur from the improper disposal of paper records. This was demonstrated several years ago when a newspaper reporter found a law firm’s old client files in a dumpster in downtown New York City. The files pertained to personal injury lawsuits, and included names and medical information of individuals as well as Social Security numbers and other personal details. Reportedly, in preparation for an office move, the law firm had hired a disposal company, but that vendor improperly dumped the records rather than shred them. This incident and many others involving improper disposal of paper records containing Personal

⁴⁴ Some of these types of incidents may generate claims under different types of insurance coverages than are typically involved in breaches involving Personal Information, depending on the nature of the breach, the damages, the claim, and the type of policy and its terms and exclusions. See section on Potential Insurance Coverage for Data Breaches, below.

⁴⁵ Alistair MacDonald and Daniel Michaels, *U.K. Touts Cybersecurity Capability*, The Wall Street Journal, October 31, 2011.

⁴⁶ *Electronic Pickpocketing*, www.wreg.com (December 3, 2010).

Information demonstrate that the improper disposal of paper files still presents a substantial exposure, and that holders of such documents need to be attentive to their disposal. This includes ascertaining the security practices of any entities to which a company delegates disposal of its records.

4. Privacy and Data Breach Concerns in Cloud Computing

As technology develops, so do new exposures, and at times they can outpace even the new regulatory requirements. Recently, there has been increasing attention on “cloud computing” and the challenges it presents to those providing it and utilizing it, in the assessment of its risks as well as its benefits, and in identifying and complying with applicable security standards and laws.⁴⁷

Although some dispute whether the concept is new, cloud computing is increasingly being used by businesses, government and individuals. In fact, on November 1, 2011, the U.S. Commerce Department’s National Institute of Standards and Technology (“NIST”) released for public comment a draft “roadmap” designed to foster federal agencies’ adoption of cloud computing, support the private sector, improve the information available to decision-makers and facilitate the continued development of the cloud computing model.⁴⁸ This could prove to be a significant accelerator of adoption of cloud services. Such increased use of cloud computing has raised significant privacy and data breach concerns.

Cloud computing has been defined as having the following essential characteristics:

- On-demand self-service – a consumer can self provision;
- Broad network access – capabilities are widely available over a network through heterogeneous devices, such as phones, computers and tablets;
- Resource pooling – a provider’s computing resources are pooled to serve multiple consumers (customers) using a multi-tenant model;
- Rapid elasticity – capabilities can be elastically provisioned and released;
- Measured service – cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts).⁴⁹

NIST defines three ways cloud services are offered:

⁴⁷ See, generally, Renzo Marchini, *Cloud Computing: A Practical Introduction to the Legal Issues*, November 2010.

⁴⁸ <http://www.nist.gov/itl/scd/cloud-11011.cfm>.

⁴⁹ See, generally <http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf>, as of November 3, 2011.

Software as a Service (SaaS) – the consumer uses the provider’s applications running on a cloud infrastructure. Online email and customer relationship applications are examples;

Platform as a Service (PaaS) – the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider;

Infrastructure as a Service (IaaS) – the consumer acquires processing, storage, networks, and other fundamental computing resources from the provider and is able to deploy and run arbitrary software, which can include operating systems and applications.⁵⁰

Each layer of services relies on the services below it. So, when a provider provides SaaS, it is also providing the platform and the infrastructure needed to run the software. Thus, in assessing privacy and data breach concerns “in the cloud,” it is important to understand which cloud service model is being used. Consumers and providers will have varying ability to easily control privacy and security concerns depending on which model is deployed. Frequently, the customer generally has no control over, or knowledge of, the exact location of the provided resources.

Examples of cloud computing abound in our personal lives and include platforms in which users can edit and store documents on remote servers. Such services eliminate the need to license desktop software as well as the need to store information on a local computer.

On a larger scale, businesses utilize cloud computing to address varying demands for computing resources (*e.g.*, high demands for online shopping during the holiday season), to achieve better cash flow by purchasing computing resources incrementally, and to outsource the operation and maintenance of non-core competencies.

Cloud computing potentially presents both security benefits and risks. On one hand, cloud computing service providers focus on providing computer services and therefore may be able to employ advanced and robust security techniques that would be cost-prohibitive for smaller companies to implement on their own. On the other hand, an entity using such resources inherently relinquishes some control over the data it provides to a cloud computing service provider. Because cloud resources are so easily deployed, IT personnel may not be involved in its use. When that happens, non-IT personnel may not have sufficient knowledge and sensitivity to properly use security features offered by a cloud provider. Moreover, unless limited by law or contract, the service provider can generally move the data from one server to another, which could potentially be in different states or different countries and subject to different data protection requirements than those of the location of the parties entering into the contract. This

⁵⁰ *Ibid.*

can result in Personal Information stored “in the cloud” being subject to either less protection or more stringent regulations than in the original jurisdiction.

Data Protection Authorities in countries such as Germany and Denmark have expressed skepticism regarding whether cloud computing services outside of Europe comply with EU data protection and transfer requirements.⁵¹ The French Data Protection Authority has recently launched a public “consultation” on cloud computing, in part to address cloud-specific data security issues.⁵²

In March 2011, the European Commission sought views from citizens, businesses, public administrations and other interested parties on how to fully benefit from cloud computing as part of a public consultation.⁵³ We anticipate that the European Commission will launch a European cloud computing strategy in 2012.

5. Privacy and Data Breach Concerns in Social Media

The growth of social media sites, such as Facebook, LinkedIn, Twitter and Google+, presents another set of privacy and data security challenges.⁵⁴ “Social media” refers broadly to online applications that allow users to create and exchange different types of content. In addition to social networking sites like Facebook and Twitter, the term encompasses video and photo sharing sites such as YouTube and Flickr, and news aggregators such as Digg and Reddit.

Facebook itself has seen explosive growth in its user population in recent years, and the site has over 800 million active users.⁵⁵ The aggregation of so much personal information, and the myriad uses to which that information is put by various applications, some of them created by third parties, has led to at least one class-action lawsuit. In August 2008, Facebook users filed a lawsuit in federal district court in California, charging that Facebook’s “Beacon” application, which automatically disclosed users’ movie purchases to the users’ friends, violated the Video Privacy Protection Act, a statute that protects against disclosure of video rental records.⁵⁶ In

⁵¹ See, e.g., Thilo Weichert, Independent Center for Data Protection for the German state of Schleswig-Holstein, *Cloud Computing and Data Privacy*, June 18, 2010, available at <http://www.datenschutzzentrum.de/cloud-computing/20100617-cloud-computing-and-data-privacy.pdf>; Danish Data Protection Agency, *Processing of sensitive personal data in a cloud solution*, February 3, 2011, available at <http://www.datatilsynet.dk/english/processing-of-sensitive-personal-data-in-a-cloud-solution>.

⁵² http://www.cnil.fr/la-cnill/actu-cnill/article/article/cloud-computing-la-cnill-engager-le-debat/?tx_ttnews%5BbackPid%5D=2&cHash=3e6a41303d, October 17, 2011, last visited on November 3, 2011.

⁵³ <http://europa.eu/rapid/pressReleasesAction.do?reference=IP/11/575&format=HTM>.

⁵⁴ According to a recent report, 65% of online adults and 50% of all adults use social networking websites, as compared to 8% and 5% respectively, in February 2005. Mary Madden and Kathryn Zickuhr, *65% of online adults use social networking sites*, Pew Internet & American Life Project, August 26, 2011; <http://pewinternet.org/~media/Files/Reports/2011/PIP-SNS-Update-2011.pdf>.

⁵⁵ Facebook statistics, www.facebook.com/press/info.php?statistics. Google+, which is Google’s social media site, had 40 million users one month after it launched. See *Long-Awaited Google+ Features Arriving Soon, Execs Say*, PC Magazine, October 19, 2011; <http://www.pcmag.com/article2/0,2817,2395009,00.asp#fbid=PLmTThEpB67>.

⁵⁶ *Lane v. Facebook*, Case No. 5:08-CV-03845-RS (N.D. Ca.) The case settled in March 2010.

EDWARDS WILDMAN PALMER LLP

2010, a The Wall Street Journal investigation reportedly found that some Facebook applications were distributing user information to dozens of advertising and Internet tracking companies, purportedly in violation of Facebook's own rules.⁵⁷

Software developers that create content for social media websites have also become targets for data thieves and, consequently, lawsuits. In late 2009, for example, one developer that creates online services and applications for use with social networking sites reportedly suffered a data breach in which a hacker (according to allegations contained in a complaint related to the breach) stole the email and social networking login credentials – *i.e.*, user names and passwords – of approximately 32 million people. The users had been required to provide their login credentials as part of a signup process to gain access to the developer's applications. A class action suit against the developer followed.⁵⁸

Facebook has also now reportedly become the target of subpoenas directed at information contained in user profiles, which it apparently receives in the thousands.⁵⁹ Facebook's legal department reportedly has resisted such requests for information, providing only basic subscriber information and in some instances refusing to comply on privacy grounds.⁶⁰

Some people are gaining access to user data on Facebook by a more direct route – by examining the content that users make available on their Facebook profiles. For example, workers' compensation claim investigators are reportedly examining the Facebook profiles of claimants to determine whether they are engaging in physical activity that their claimed injuries should prevent.⁶¹ Facebook content is also increasingly being used as evidence in divorce cases. In a 2010 survey by the American Academy of Matrimonial Lawyers, 80% of the responding attorneys reported observing growth in the use of such evidence.⁶²

Others have identified ways to utilize publicly available information on Facebook and other websites to obtain information about the site's users. For example, researchers at Carnegie Mellon University in Pennsylvania recently reported that they have been able to successfully guess individuals' Social Security numbers based on information on Facebook and other websites.⁶³ The researchers also claim to have developed an application for iPhones that can

⁵⁷ *Facebook In Privacy Breach*, The Wall Street Journal, October 18, 2010.

⁵⁸ *Claridge v. RockYou, Inc.*, No. C 09-6032 PJH (N.D. Ca.).

⁵⁹ Andy Furillo, *Sacramento judge delays contempt decision against Facebook*, Sacramento Bee, January 7, 2011.

⁶⁰ Amy Miller, *Facebook GC Tells Lawyers He's Looking for a Fight*, law.com, February 2, 2010.

⁶¹ Roberto Cenicerros, *Comp cheats confess all on social network sites*, businessinsurance.com, September 6, 2009.

⁶² David Gardner, *The marriage killer: One in five American divorces now involve Facebook*, Daily Mail, December 2, 2010.

⁶³ *Facebook's Privacy Issues Are Even Deeper Than We Knew*, Forbes, August 8, 2011, <http://www.forbes.com/sites/chunkamui/2011/08/08/facebooks-privacy-issues-are-even-deeper-than-we-knew/> (visited October 21, 2011). See also Face Recognition Study – FAQ, <http://www.heinz.cmu.edu/~acquisti/face-recognition-study-FAQ/> (visited October 21, 2011).

take a photograph of someone, and through the use of facial recognition software, display on-screen that person's name and vital statistics.⁶⁴ Additionally, they reportedly looked at photographs of anonymous people (many of whom used pseudonyms) on a dating website and, through facial recognition software and Facebook, were able to identify about 10% of the dating site's members.

The increased use of social media in the workplace adds another layer of complexity to privacy issues. In 2010, the United States Supreme Court decided that a public employee who uses an employer-supplied, text messaging-enabled pager device does have a reasonable expectation of privacy with regard to personal messages sent on the device. The Court ruled, however, that under a Fourth Amendment analysis, the employer's review of two months' worth of the employees' text messages (in order to determine whether they were exceeding their allowable quotas for personal text messages) was justified.⁶⁵ Presumably, the Court's holding would also apply to messages shared on social media websites via employer-provided hardware.

In another instance of the intersection between employment law and social media, in November 2010, the National Labor Relations Board filed a lawsuit against an ambulance company, alleging that it violated federal labor laws (specifically, an employee's right to engage in protected concerted activities with other employees pursuant to the National Labor Relations Act⁶⁶) when it fired an employee for posting unflattering comments about her supervisor on a Facebook page.⁶⁷ The parties settled in January 2011; the employer agreed, among other things, to amend its social media policy.⁶⁸

In a similar vein, employment background checks can include information from credit reports, employment and salary history, criminal records, and social media. According to the FTC, the same rules that apply to other types of information also apply to social media. For example, the FTC website reports that FTC staff recently looked at a company selling background information from social media to see if they were complying with the Fair Credit Reporting Act ("FCRA"), and noted that "companies selling background reports must take reasonable steps to ensure the maximum possible accuracy of what's reported from social networks and that it relates to the correct person," as well as comply with other FCRA sections.⁶⁹

⁶⁴ *Face-matching with Facebook profiles: How it was done*, C/NET News, August 4, 2011, http://news.cnet.com/8301-31921_3-20088456-281/face-matching-with-facebook-profiles-how-it-was-done/

⁶⁵ *City of Ontario, California v. Quon*, 130 S. Ct. 2619, 560 US ___, 177 L. Ed. 2d 216 (June 17, 2010).

⁶⁶ 29 U.S.C. § 151 *et seq.*

⁶⁷ *American Medical Response of Connecticut, Inc. and International Brotherhood of Teamsters, Local 443*, Case No. 34-CA-12576 (NLRB Region 34).

⁶⁸ *Conn. ambulance co. settles Facebook firing case with Labor Board*, International Business Times, Feb. 16, 2011 (<http://www.ibtimes.com/articles>)

⁶⁹ Lesley Fair, *The Fair Credit Reporting Act & social media: What business should know*, FTC Business Center Blog, June 23, 2011 (<http://business.ftc.gov/blog/2011/06/fair-credit-reporting-act-social-media-what-businesses-should-know>); Letter

Potentially problematic uses of social media have been reported outside the employment context as well. In a recently reported incident, a physician revealed sufficient information about a patient on Facebook to constitute a breach of patient privacy.⁷⁰ Judges and lawyers have been sanctioned for communications through social media,⁷¹ and an Israeli army mission was aborted in 2010 when a soldier revealed the mission on Facebook.⁷²

The use of social media is likely to continue to expand. Banks and lenders are expected to incorporate social media conversations into their analysis of credit risk.⁷³ For example, some online comments may be interpreted by lenders as an indicator that the applicant may be delinquent on a future loan or a possible credit risk. Research is reportedly being conducted to try to create correlations between online (social media) comments and possible credit issues, which could lead to a form of “social media underwriting” in the future.

These are just the tip of the iceberg for privacy issues arising from social media. Social media is certain to present increasing challenges to privacy and data security..

6. Privacy Issues Arising Out of Behavioral Advertising and On-Line Tracking

Targeted advertising has become ubiquitous. Digital advertising is an \$80.2 billion industry.⁷⁴ Significant privacy concerns have recently been raised by regulators and in a rash of class actions arising from targeted advertising and tracking of consumer behavior by companies that market online and via mobile devices.

a. In the United States

(i) The FTC Recommendations

The FTC defines Online Behavioral Advertising (“OBA”) as a process of “tracking consumers’ activities online to target advertising.”⁷⁵ It often, but not always, includes a review of the searches consumers have conducted, the Web pages visited, the purchases made, and the content viewed, in order to deliver advertising tailored to an individual consumer’s interests. In its December 2010 report titled “Protecting Consumer Privacy in an Era of Rapid Change: A

from Maneesha Mithal, Associate Director of the Division of Privacy and Identity Protection, Bureau of Consumer Protection, Federal Trade Commission; to Renee Jackson, dated May 9, 2011 (<http://ftc.gov/os/closings/110509socialintelligenceletter.pdf>).

⁷⁰ Chelsea Conaboy, *For doctors, social media a tricky case*, Boston Globe, April 20, 2011

⁷¹ See, e.g., *Judge resigns amid probe about Facebook friend*, Atlanta Journal-Constitution, January 7, 2010.

⁷² *Israeli military calls off raid after soldier posts details*, cnn.com. March 3, 2010.

⁷³ Ken Lin, *What Banks and Lenders Know About You from Social Media*, Mashable Social Media, October 7, 2011 (<http://mashable.com/2011/10/07/social-media-privacy-banks/>).

⁷⁴ www.emarketer.com (June 2011). Digital spending is expected to exceed \$94 billion in 2012. *Id.*

⁷⁵ FTC Staff, *FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising* (Feb. 2009), at p. 2 (<http://www.ftc.gov/os/2009/02/P0085400behavadreport.pdf>).

Proposed Framework for Businesses and Policymakers,” the FTC proposed a “Do Not Track” option to prevent targeted advertising without consumer consent. The final guidance is expected shortly.

In 2011, the FTC announced three enforcement consent orders against companies for delivering OBA without consumer consent. For each of these actions, the FTC alleged “deceptive” acts in violation of the FTC Act and imposed ongoing reporting requirements for 20 years.⁷⁶

(ii) Do Not Track Class Actions

Consumers are claiming that tracking their activities online or on their mobile devices violates their right to privacy, and generally allege a variety of state and federal statutory and common law claims and violations. The class action bar filed more than 80 putative class action lawsuits in 2011, alleging violations of the Electronic Communications Privacy Act (ECPA), the Computer Fraud and Abuse Act (CFAA), and state laws.

The ECPA prevents access and tracking of user behavior without consent. Some courts have shown a willingness to infer consent if a consumer has reviewed a privacy policy that discloses tracking.⁷⁷ The CFAA makes it unlawful to track user browsing behavior if this causes \$5,000 in economic loss. Where economic harm is not specified, Courts have been willing to dismiss CFAA complaints.⁷⁸

(iii) Federal and State Do Not Track Legislation

On March 16, 2011, the Obama administration called for a universal privacy bill, and specifically supported the FTC’s “Do Not Track” proposals. Legislators have responded. As of

⁷⁶ *In the Matter of Chitika, Inc.*, the FTC pursued Chitika for having an “opt-out” for behavioral advertising that expired after 10 days, alleging that this was a “deceptive” practice because the opt-out was not meaningful. Chitika now has a 20-year reporting requirement to the FTC. In August 2011, the FTC pursued its first mobile app complaint, resulting in a consent decree against a mobile advertiser that served targeted ads to children under the age of 13 in violation of COPPA. *United States of America, Plaintiff v. W3 Innovations, LLC, also d/b/a Broken Thumbs Apps* <http://www.ftc.gov/opa/2011/08/w3mobileapps.shtm>. Most recently, on November 8, 2011, the FTC entered into a consent order against a digital third-party advertiser, Scanscout, for its alleged use of flash cookies to target advertising.

⁷⁷ *See e.g., Mortensen v. Bresnan Communications LLC*, 1:10-cv-00013 (D. Montana) (December 2010 Order, Dkt. 30 at p. 12, dismissing plaintiffs’ class action allegations based upon the federal ECPA on grounds that Bresnan’s privacy disclosures disclosed its collection and tracking of user “browsing behavior” and concluding that by using “... Bresnan’s Internet Service, ... [plaintiffs] gave or acquiesced their consent to such interception.”); and *In re Facebook Privacy Litigation* (N. D. Cal.) (where on May 12, 2011, Judge Ware dismissed the plaintiffs’ ECPA claims with leave to amend); and *In re Facebook Privacy Litigation* (N.D. Cal. November 22, 2011) (where J. Ware dismissed the plaintiffs’ claims with prejudice on the ground, among other things, that no harm had been shown).

⁷⁸ *See e.g., In LaCourt v. Specific Media, Inc.* 2011 WL 1661532 (C.D. Cal. Apr. 28, 2011), the court held that plaintiffs failed to allege economic harm as required by the CFAA. Similarly, in *Bose v. Interclick; McDonald’s USA, LLC; McDonald’s Corporation; CBS Corporation; Mazda Motor of America, Inc. and Microsoft Corporation*, Case No. 1:10-cv-9183 (S.D.N.Y. August 2011), the court dismissed with prejudice the plaintiff’s claims of alleged violations of the CFAA for failure to allege harm. *See Order, Dkt. 36 dated August 17, 2011*. *See also, In Re iPhone App. Litigation* 11-MD-02250-LHK, Order Granting Defendants’ Motions to Dismiss for Lack of Article III Standing With Leave to Amend, Dkt. 8 (N.D. Cal. September 20, 2011).

EDWARDS WILDMAN PALMER LLP

December 2011, there are three privacy bills that address tracking in the House of Representatives and two bills in the Senate.⁷⁹ California has proposed a “Do Not Track” bill that contains a private right of action and statutory penalties.⁸⁰

On September 15, 2011, the FTC recommended amendments to the Children’s Online Privacy Protection Act (“COPPA”)⁸¹ which would expand the definition of “personal information” to include OBA information.

b. E.U. Positions on Online Behavioral Advertising

Effective May 25, 2011, countries in the EU were required to implement regulations to obtain explicit consent before companies collect OBA information. On December 13, 2011, the UK’s Information Commissioner’s Office advised that opt-in consent will be necessary to collect OBA.⁸²

c. Canada

Canada’s Office of the Privacy Commissioner (“OPC”) issued its guidance on OBA and tracking in December 2011. It takes the position that OBA “generally” constitutes personal information,⁸³ and that disclosures “cannot be buried in a privacy policy,” nor should OBA be collected from children. If declining cookies “renders a service unusable, then organizations should not be employing that type of technology.”

d. Upcoming

In light of the importance of digital advertising revenue to digital business models, the issue of tracking and privacy will continue to grow in 2012, as will concomitant regulatory scrutiny,

⁷⁹ H.R. Bill Nos. 611, 653 and 654, recommend “do not track” without consumer consent (introduced by Representatives Jackie Speier and Bobby Rush in February 2011). Also, Senators John Kerry and John McCain introduced similar legislation on the Senate side. See Commercial Privacy Bill of Rights Act (introduced March 2011) at <http://kerry.senate.gov/imo/media/doc/Commercial%20Privacy%20Bill%20of%20Rights%20Text.pdf>. Senator Rockefeller introduced the [Do-Not-Track Online Act of 2011](#) (which would create a “universal legal obligation” for companies to honor users’ opt-out requests on the Internet and mobile devices).

⁸⁰ In California, a “do not track” bill is pending. The bill, SB 761, was introduced by state Senator Alan Lowenthal in April 2011. It would require the state attorney general to issue regulations that would require Web companies to notify state residents about online data collection and allow them to opt out. In addition, the California bill contains a private right of action and \$1,000 statutory penalty per violation.

⁸¹ Children’s Online Privacy Protection Rule 16 C.F.R. § 312 (located at <http://www.ftc.gov/os/2011/09/110915coppa.pdf>). Comments were originally due on November 28, 2011 but the comment period was extended to Friday December 23, 2011 <https://ftcpublic.commentworks.com/ftc/2011coppauleview/>. Also, on November 8, 2011, the FTC issued its new guidance regarding consumers and cookies. See <http://onguardonline.gov/articles/0042-cookies-leaving-trail-web>.

⁸² Must Try Harder on Cookie Compliance Says ICO, http://www.ico.gov.uk/news/latest_news/2011/must-try-harder-on-cookies-compliance-says-ico-13122011.aspx.

⁸³ Guidelines located at http://www.priv.gc.ca/information/guide/2011/gl_ba_1112_e.pdf.

legislative initiatives, and legal proceedings. With over 80 class actions filed by December 2011, 2012 is likely to see similar actions filed against companies in a broad range of industries.

7. New Technologies Bring New Risks

As corporations and consumers embrace new technology, cyber criminals adapt their tactics to take advantage of new opportunities for data theft. Reportedly, sales of smartphones recently eclipsed sales of PCs, and cyber criminals are beginning to shift more of their attention to trying to exploit security holes in the ubiquitous mobile devices – particularly as PC security has recently been improving.⁸⁴ According to one mobile security firm, the number of Android applications infected with malware increased 250% from January to June of 2011, and up to one million Android users were hit with malware in the first six months of 2011.⁸⁵ While malware installation on smartphones currently requires users to take some action, such as clicking on a link, security experts warn that automated attacks could become a reality.⁸⁶

8. The Breadth of the Problem

The costly and growing exposure presented by data breaches is demonstrated by the following recently reported statistics.

a. The Big Picture: Number of Breaches and Associated Costs

- As of November 1, 2011, 340 breaches had been reported and over 22 million records had been exposed in 2011.⁸⁷
- The average total cost of a data breach per company was more than \$7.2 million in 2010,⁸⁸ which equates to an average cost of \$214 per record compromised. In 2010, over 60% of the total cost of a data breach was attributed to business lost as a result of the breach.⁸⁹
- Costs based on claims payout data submitted by insurers of 77 covered breaches that occurred between 2005 and 2010 were of an average cost for a data breach of

⁸⁴ Riva Richmond, *Security to Ward Off Crime on Phones*, The New York Times, February 23, 2011.

⁸⁵ Paul Wagenseil, *Android Malware Shoots Up 250 Percent in Six Months*, Security News Daily, Aug. 3, 2011; <http://www.securitynewsdaily.com/android-malware-shoots-up-1021/>. Android phones have been targeted by malware much more than iPhones and other mobile phone operating systems. McAfee: *Android Malware Surges 76%, iPhone Untouched*; Electronista, Aug. 23, 2011; <http://www.electronista.com/articles/11/08/23/mcafee.shows.android.facing.huge.spike.in.malware/>.

⁸⁶ *Security to Ward Off Crime on Phones*, *supra*.

⁸⁷ <http://www.idtheftcenter.org/IIRC%20Breach%20Report%202011.pdf>. This did not include the Sony breach that purportedly involved over 100 million records, although not all apparently included PI.

⁸⁸ Ponemon Institute, LLC, *2010 Annual Study: U.S. Cost of a Data Breach*.

⁸⁹ *2010 Annual Study: U.S. Cost of a Data Breach*, *supra*.

\$2.4 million, with the average cost per record of \$5.00; the typical number of records exposed was 100,000 with the average number 1.7 million; the average cost for legal defense was \$500,000, and for legal settlement was \$1 million; and for crisis services (including forensics, notification, call center and legal counsel related to that) was \$800,000.⁹⁰

- One in five companies faced their first data breach in 2010, and these “first time” breaches cost 48% more than subsequent breaches, suggesting that experience may help companies become more efficient at managing costs.⁹¹
- 88% of organizations that participated in one survey suffered at least one data breach in 2010, up slightly from 2009.⁹²
- The total economic burden created by data breaches in the healthcare industry is nearly \$6 billion annually.⁹³

b. The Industries, Assets, and Types of Data Most Frequently Compromised

- The three main industries affected by data breaches in 2010 were: hospitality (40%); retail (25%); and financial services (22%).⁹⁴
- Of the various types of assets compromised in 2010, ranging from desktop computers to automated teller machines, one study found that point-of-sale (POS) servers were most frequently breached (36%) and resulted in the largest percentage of compromised records (28%).⁹⁵
- The types of data most frequently compromised in 2010 were: (1) payment card data/ numbers (78% of breaches and 96% of records); (2) authentication credentials (45% of breaches and 3% of records); and (3) personal information

⁹⁰ NetDiligence, *CyberLiability & Data Breach Insurance Claims: A Study of Actual Payouts for Covered Data Breaches*, June 2011.

⁹¹ *2010 Annual Study: U.S. Cost of a Data Breach*, *supra*.

⁹² *2010 Annual Study: U.S. Enterprise Encryption Trends*, The Ponemon Institute, November 2010.

⁹³ Deloitte, *Issue Brief: Privacy and Security in Health Care: A fresh look (2011)*.

⁹⁴ *2011 Data Breach Investigations Report*, A study conducted by the Verizon RISK Team in cooperation with the United States Secret Service and the Dutch High Tech Crime Unit; the NetDiligence survey of insurer data of breach events occurring between 2005 and 2010 also reported that more than 60% of breaches in their sampling occurred in the financial services, healthcare and retail sectors. NetDiligence, *Cyber Liability & Data Breach Insurance Claims*, *supra*.

⁹⁵ *2011 Data Breach Investigations Report*, *supra*.

such as name, address and Social Security number (15% of breaches and 1% of records).⁹⁶

c. Causes

- According to one study, 92% of attacks in 2010 were not considered highly difficult, and 96% of breaches were avoidable through simple or intermediate controls. Additionally 89% of the breached companies that were subject to Payment Card Industry Data Security Standards (PCI-DSS) had not achieved compliance with them.⁹⁷
- One study reported that negligence remains the most frequent cause of data breaches, and that breaches caused by malicious attacks surpassed those caused by system failures in 2010 for the first time in the study's history.⁹⁸ The study reported that breaches caused by malicious attacks cost 48% more than breaches caused by negligent insiders or system glitches.⁹⁹
- According to another major study, external threat agents caused or contributed to 92% of data breaches in 2010. Such external agents include lone hackers, organized crime groups, and government entities.¹⁰⁰
- Thirty-nine percent of breaches in 2010 involved mistakes by third-party outsourcers or consultants, and those breaches cost 48% more than internal breaches.¹⁰¹
- In 2010, 35% of breaches involved lost or stolen laptop computers or other mobile data-bearing devices, which breaches cost 26% more than breaches not involving such devices.¹⁰²
- The number of malware and spyware programs that had been installed on mobile phones more than doubled from December 2009 to May 2010.¹⁰³

⁹⁶ 2011 Data Breach Investigations Report, *supra*.

⁹⁷ 2011 Data Breach Investigations Report, *supra*.

⁹⁸ 2010 Annual Study: U.S. Cost of a Data Breach, *supra*.

⁹⁹ 2010 Annual Study: U.S. Cost of a Data Breach, *supra*.

¹⁰⁰ 2011 Data Breach Investigations Report, *supra*.

¹⁰¹ 2010 Annual Study: U.S. Cost of a Data Breach, *supra*.

¹⁰² 2010 Annual Study: U.S. Cost of a Data Breach, *supra*.

¹⁰³ Riva Richmond, *Security to Ward Off Crime on Phones*, The New York Times, Feb. 23, 2011; http://www.nytimes.com/2011/02/24/technology/personaltech/24basics.html?_r=1.

- Malware targeting Android mobile operating systems reportedly increased 472% in volume between May and November 2011.¹⁰⁴
- The most common threat actions involved in 2010 breaches were (1) hacking, (2) malware, (3) physical (threats that employ physical action and/or require physical proximity), (4) misuse (*e.g.*, embezzlement, skimming, and abuse of system access) and (5) social (*e.g.*, bribery, forgery, and phishing).¹⁰⁵

d. Breach Discovery and Response

Reports of 2010 breaches provide the following information about the discovery of and response to data breaches:

- Eighty-six percent of breaches were discovered by an external party, while only 6% were detected by internal measures designed and deployed to detect such incidents, and 5% were discovered internally in a passive manner (*e.g.*, an employee notices something awry).¹⁰⁶
- It was a matter of months before 36% of the breaches were discovered. Thirty-eight percent of breaches were discovered in a matter of weeks, and 17% were discovered in a matter of days.¹⁰⁷
- Forty-three percent of companies reportedly notified victims within one month of discovering a data breach, marking a significant increase in “rapid responders” since 2009. These quick responders, however, paid 35% more per record in breach costs,¹⁰⁸ indicating that a thoughtful, unrushed response is important in responding to a breach and avoiding cost inefficiencies.

The reality is that any entity that obtains, maintains or transmits Personal Information of employees, customers, clients, or any other third party is potentially exposed to a data breach and the related costs. These costs include direct expenses such as engaging forensic experts, obtaining legal advice as to required notifications, providing notifications and outsourced hotline support, offers of free credit monitoring subscriptions and identity theft insurance and discounts for future products and services, payment of fines imposed, and the defense and resolution of

¹⁰⁴ Gregg Keizer, *Android malware explodes, jumps five-fold*, Computer World, November 18, 2011, at www.computerworld.com.

¹⁰⁵ *2011 Data Breach Investigations Report, supra*.

¹⁰⁶ *2011 Data Breach Investigations Report, supra*.

¹⁰⁷ *2011 Data Breach Investigations Report, supra*. The determination of the exact time that a breach occurs is often a significant forensic issue, particularly with regard to malicious hackings, as such breaches often involve malware installed months or even years before it is activated.

¹⁰⁸ *2010 Annual Study: U.S. Cost of a Data Breach, supra*.

third-party claims, as well as the indirect costs of in-house time spent addressing the breach and supporting the resulting investigations, the damage to reputation, and the loss of customers, business and related revenue.

9. The Importance of Timely and Proper Notification

A poorly executed breach response can harm a company's reputation and increase its out-of-pocket costs, including exposure to fines and lawsuits arising from non-compliance with data security laws and regulations.

In one study, 83% of consumers surveyed reported receiving a data breach notification during the 24 months prior to the survey, while 55% had been notified of two or more data breaches.¹⁰⁹ The study found that 63% of the respondents said that the notification letters they received offered no direction on the steps consumers should take to protect their personal information and, as a result, 31% terminated their relationships with the organization and 57% said they had lost trust and confidence in the organization. Over half of the respondents rated the timeliness, clarity, and quality of the breach notification as only poor-to-fair.¹¹⁰

Moreover, as noted above, one recent study noted that quick responders on average paid 35% more per record in breach costs, indicating that a thoughtful, unrushed response is important in responding to a breach and avoiding cost inefficiencies and the potential need to supplement notifications with resulting cost duplications.¹¹¹

These statistics reinforce the importance of companies having a good response plan in place before a breach occurs so that they can address a breach promptly and properly should one occur. This is critical both to maintaining regulatory compliance, and to minimizing the negative impact on customer relationships and business reputation.

Further, lawsuits arising from data breaches often include causes of action alleging that the breached company failed to timely notify customers and others whose personal information was compromised by the breach, proximately causing damages that allegedly would have been avoided or minimized with a more timely response. Moreover, recent regulatory investigations of data breaches have often focused on the length of time a company that sustained a breach took to notify those affected by the breach.¹¹²

¹⁰⁹ Dr. Larry Ponemon, *Consumer's Report Card on Data Breach Notification*, April 15, 2008.

¹¹⁰ *Id.*

¹¹¹ *2010 Annual Study: U.S. Cost of a Data Breach, supra.*

¹¹² *See, e.g.,* discussion of Health Net and Anthem Blue Cross and Blue Shield breaches and the investigations of them by the Connecticut Attorney General, *infra.*

Thus, having a breach response plan in place is likely to enable a company to respond to a breach both appropriately and within a reasonable time frame, and support a company's legal defense against third-party lawsuits as well as regulatory investigations arising from the breach.

II. The Regulatory and Statutory Landscape: Obligations Under Data Privacy and Security Laws and Regulations

The regulatory landscape related to data privacy and security has changed significantly in the past decade in response to increasing concern about data breaches, identity theft, and fraud. State, federal, industry, and international requirements impose new and evolving obligations on companies to institute information security plans in advance of a breach, as well as notification requirements after a breach occurs. Non-compliance with applicable requirements raises regulatory issues including fines and penalties, as well as liability to third parties whose information is accessed due to a data breach or who otherwise sustain financial loss or other damages as a direct result of a breach. Non-compliance with regulatory and legal requirements can be used as evidence of departure from the standard of care in third-party claims against a company whose data systems were breached.

Although laws and regulations concerning data privacy and security generally do not create a private right of action, the failure to comply with such requirements is usually asserted in third-party lawsuits as evidence of inadequate security, particularly when the company's privacy notice represents that it is in compliance with applicable legal and regulatory requirements.¹¹³

1. State Data Privacy and Security Requirements

In an effort to reduce the risk of identity theft, many states have enacted laws, and many state regulatory bodies have promulgated regulations, that impose obligations on entities that obtain and/or maintain Personal Information of individuals. These laws and regulations are intended to protect Personal Information and, in the event of a breach, to require notification to those individuals whose Personal Information has been or may have been subject to unauthorized access or acquisition.

a. Protection of Social Security Numbers

Social Security numbers have become a prime target of data thieves. Unlike debit and credit card numbers, social security numbers are difficult to change and can be used to obtain additional documentation used in identity theft for purposes other than a discrete number of fraudulent transactions. Recent reports indicate that hackers are focusing on the Social Security numbers of children, which are generally not yet in use by the holders to obtain credit and thus

¹¹³ See, e.g., *Daly v. Metropolitan Life Ins. Co.*, 4 Misc. 3d 887, 782 NYS 2d 530 (2004); *Amburgy v. Express Scripts, Inc. et al.*, Civil Docket 4:09-CV-00705-FRB, filed May 2009 in the U.S. District Court, Eastern District of Missouri; *Alison v. Aetna, Inc.*, filed in June 2009 in the U.S. District Court, Eastern District of Pennsylvania. Complaints in these actions cited non-compliance with the companies' privacy notices.

are not associated with a tarnished credit history.¹¹⁴ Breaches involving Social Security numbers are also of concern to law enforcement agencies charged with state and national security, due to their ability to be used as identification for purposes well beyond fraudulent financial transactions, including false identification to law enforcement and national security authorities.

Many states impose specific requirements governing the handling of Social Security numbers. For example, in October 2008, Connecticut enacted a law that requires any person or entity that collects Social Security numbers to create a protection policy specifically related to Social Security numbers.¹¹⁵ The company policy, which must be published or publicly displayed (such as on the company's website), must protect confidentiality, prohibit unlawful disclosure, and limit access to Social Security numbers. Similarly, the New York Social Security Number Protection Law prohibits businesses from, among other things, making a Social Security number available to the general public, intentionally or not; printing a Social Security number on any card or tag required for an individual to access products, services or benefits; or requiring an individual to transmit a Social Security number over the Internet, unless the Internet connection is secure.¹¹⁶ Other states have enacted similar laws and regulations to protect the Social Security numbers and other personal information of their residents.¹¹⁷

b. Record Disposal Requirements

Many states also regulate the disposal of records containing Personal Information. For example, under Massachusetts and New York law, records with Personal Information must be redacted, burned, pulverized, shredded or destroyed in some other way that will render the data unreadable. In Massachusetts, if third parties are contracted to dispose of such records, they must implement policies and procedures that prohibit unauthorized access to or use of Personal Information during collection, transport and disposal. Both states impose fines for noncompliance.¹¹⁸

Companies disposing of records containing Personal Information also need to consider whether they are subject to federal provisions with disposal requirements. The Fair and Accurate Credit Transactions Act of 2003, for example, requires businesses and individuals that use consumer reports, such as lenders, insurance companies, employers, landlords, car dealers, and debt collectors, to properly dispose of those consumer reports.¹¹⁹

¹¹⁴ *Thieves target children's Social Security numbers*, Chicago Sun-Times, August 3, 2010.

¹¹⁵ Conn. Gen. Stat. § 42-471.

¹¹⁶ N.Y. Gen. Bus. Law § 399-dd.

¹¹⁷ *See, e.g.*, Cal. Civ. Code § 1798.85; Mich. Comp. Laws § 445.84; Or. Rev. Stat. § 646A-620; Tex. Bus. & Com. § 501.

¹¹⁸ Mass. Gen. Law ch. 93I § 2; N.Y. Gen. Bus. Law § 399-h.

¹¹⁹ 15 U.S.C. § 1681w(a)(1); *see also* 69 Fed. Reg. 68690-01 (Nov. 24, 2004) codified at 16 C.F.R. § 682.

c. Data Breach Notification Requirements

In the event of a data breach involving unauthorized access of Personal Information, state laws and regulations in most U.S. jurisdictions mandate notice of the breach to affected individuals, and some states also require reporting to regulatory agencies and attorneys general. Often, vast numbers of individuals can be involved in a single breach, and large breaches usually involve residents of many jurisdictions.

Fifty U.S. jurisdictions, including 46 states, the District of Columbia, Guam, Puerto Rico and the U.S. Virgin Islands, have enacted data breach notification laws.¹²⁰ These laws specify the steps that a company must take in response to a breach that affects its residents. Although the data breach notification laws of each of the 50 jurisdictions are similar, they are not identical. In the event of a breach or potential breach of data security, a company must carefully review the requirements of each applicable jurisdiction to determine its obligations in that particular jurisdiction.¹²¹

In addition to these requirements, as discussed below, various state departments of insurance have also issued separate requirements mandating notification of data breaches to the states' insurance commissioners.¹²²

In the event of a data breach, an initial, and major, task is to identify which jurisdictions' requirements apply. Entities often find themselves subject to the different, sometimes conflicting, requirements of multiple jurisdictions. A single data breach incident may take place in only one state insofar as the location at which the entity's data security was breached. Nevertheless, individuals affected by the breach may reside in many different states and other jurisdictions, and the company will likely need to comply with the data breach requirements of many of those jurisdictions. For example, if a laptop is stolen from or lost in an office in Texas, and that laptop contains the Personal Information of Maine, Massachusetts, New Hampshire and Vermont residents, the data breach laws of Maine, Massachusetts, New Hampshire and Vermont, as well as Texas, may be triggered. When the issue is a breach of a database or loss of computerized records containing information of individuals residing in different locations, the notification requirements of all U.S. states and other jurisdictions with such requirements are potentially triggered.

Typically, the applicability of notice requirements of a given jurisdiction depends on several factors: (i) whether the type of information that has been lost, stolen or misplaced fits the jurisdiction's definition of "personal information;" (ii) whether there has been a "breach of the

¹²⁰ As of November 2011, the states that do not yet have such notification laws are Alabama, Kentucky, New Mexico and South Dakota.

¹²¹ A list of jurisdictions and links to their data breach notification laws are available at <http://www.ncsl.org/programs/lis/cip/priv/breachlaws.htm>.

¹²² See section on Exposure of Companies in the Insurance Industry as Entities Subject to Data Breaches, *infra*.

security of the system” under the jurisdiction’s definitions and requirements; (iii) whether the incident meets a threshold of harm or likelihood of harm; and (iv) whether the requisite number of individuals whose Personal Information was accessed are residents of the state. Not all jurisdictions have the same definitions or triggers. For example, some states provide for notification if there is unauthorized “acquisition” of Personal Information, while others may require only unauthorized “access” to Personal Information; some states have a harm threshold, and some do not.

The data breach notification statutes of each relevant jurisdiction must also be considered to determine whether:

1. Residents of the jurisdiction must be notified;
2. Notices to affected individuals must contain specific content (or are prohibited from containing certain information, as some states, such as Massachusetts, do not want publication of the methodology of the breach or the type of information at risk, while others require the disclosure of such information);
3. State attorneys general and other state agencies must be notified, and if so whether those notices must contain specific content and be provided before notification of affected individuals; and
4. Consumer reporting agencies, such as Experian, TransUnion and Equifax, must be notified.

Certain states, including Maryland, New Hampshire, New York, North Carolina, and Vermont, require that notices to affected individuals include specific content. These states typically require that the notice contain the following:

- Details regarding how, where and when the breach occurred;
- Types of Personal Information that were lost, misplaced or stolen;
- Contact information of the major credit reporting agencies;
- The company’s contact information; and
- Advice on remaining vigilant by reviewing account statements and credit reports.

In contrast, Massachusetts *prohibits* the disclosure of two of the above-listed categories of information: the mechanism of the breach, and the types of information affected.

As the specific content requirements for notice of breach varies from state to state, it is important for the company that experienced a data breach to ascertain which states’ notice requirements are triggered, and the requirements of each particular state as applied to the situation at hand. As

noted above, in the U.S., most, but not all, data breach notification requirements apply to breaches of Personal Information in electronic or computerized format, but not to Personal Information contained in paper documents. Often, more than one state's notice requirements will be triggered.

d. Massachusetts is at the Forefront in Data Privacy and Security Regulation and is Setting a New Standard

Massachusetts, through its Office of Consumer Affairs and Business Regulation (“OCABR”), has promulgated one of the most comprehensive regulatory schemes for data privacy and security, which went into effect March 1, 2010, and has set the new U.S. standard for data protection.

The Massachusetts data security regulation (201 C.M.R. 17.00, the “Massachusetts Regulation”) applies to any individual or company, regardless of type, size or location, that possesses or uses Personal Information of Massachusetts residents. Under the Massachusetts Regulation, Personal Information includes the name of a Massachusetts resident together with his or her Social Security number, driver's license, financial account, or credit card numbers (with or without PIN). Any entity, including insurance companies, producer entities and service providers, that uses or stores the Personal Information of Massachusetts residents, whether of employees, insureds, beneficiaries or claimants, is subject to the Massachusetts Regulation.¹²³

The Massachusetts Regulation establishes the most rigorous data security requirements in the U.S. to date. It focuses to a large extent on what recently has been a target of both cyber criminals and inadvertent breaches due to lost devices: electronic information in transit and information stored on laptops and PDAs. To comply, companies are required to have developed and adopted by March 1, 2010 a comprehensive written information security program (referred to as a “WISP”) that satisfies the specific requirements of the Massachusetts Regulation, including the following:

- Identify and evaluate internal and external risks;
- Regularly monitor employees' access to Personal Information;
- Prevent terminated employees from accessing documents, devices and other records that contain Personal Information;
- Take reasonable steps to select and retain third-party service providers that are capable of compliance with the Massachusetts Regulation;

¹²³ The extraterritorial authority of the OCABR and the Massachusetts Attorney General to enforce the Massachusetts Regulation against companies located outside Massachusetts borders is yet to be fully tested.

- Review security measures annually, and update the WISP when there is a material change in business operations;
- Develop and maintain a procedure for actions to take in response to any breach of security;
- Train employees about and discipline employees for violation of the policy; and
- Designate one or more employees to maintain, supervise and implement the WISP.

The WISP must also address the establishment and maintenance of a detailed computer security program as to Personal Information of Massachusetts residents, including, to the extent technically feasible:

- Encryption of all transmitted records and files containing Personal Information that are stored on laptops and other portable devices and/or will travel across public networks or wirelessly;
- User-authentication protocols and access-control measures, including control over user identifiers, passwords and access;
- A system for monitoring unauthorized use; and
- Up-to-date firewalls, anti-virus definitions and anti-malware programs.

The OCABR extended the effective date several times, and announced amendments, before the final effective date of March 1, 2010. Prior to the effective date, the OCABR announced amendments to (i) clarify the risk-based approach to the Massachusetts Regulation, (ii) coordinate the requirements for third-party vendors with similar requirements of federal law, and (iii) require appropriate encryption technology to the extent technically feasible. The OCABR also offered further guidance through additional Frequently Asked Questions (“FAQs”) issued with the amendments.¹²⁴

In an effort to ease the burden on small businesses, the OCABR amended the Massachusetts Regulation to make clear that the Massachusetts Regulation is risk-based in both implementation and enforcement, stressing that there is no one-size-fits-all WISP. The Massachusetts Attorney General will judge compliance on a case-by-case basis to take into account the following factors: (i) the size, scope and type of business handling the information; (ii) the amount of resources

¹²⁴ The FAQs and other guidance related to the Massachusetts Regulation are available at: <http://www.mass.gov/?pageID=ocatopic&L=3&L0=Home&L1=Business&L2=Identity+Theft&sid=Eoca>.

EDWARDS WILDMAN PALMER LLP

available to the business; (iii) the amount of stored data; and (iv) the need for security and confidentiality of both consumer and employee information.

This risk-based approach brings the Massachusetts Regulation in line with both the enabling legislation and applicable federal law, including two rules promulgated by the FTC: (i) the Red Flags Rule that requires creditors and financial institutions to have a written Identity Theft Prevention Program to detect warning signs of identity theft and fraud; and (ii) the Gramm-Leach-Bliley Safeguards Rule (16 C.F.R. Part 314), which requires financial institutions to have a security plan to protect personal consumer information (both discussed below).

The Massachusetts Regulation also requires that companies oversee their third-party vendors by:

- (i) Taking reasonable steps to select and retain third-party service providers that are capable of maintaining appropriate security measures to protect such Personal Information consistent with these regulations and any applicable federal regulations; and
- (ii) Requiring by contract that such third-party service providers implement and maintain such appropriate security measures for Personal Information.

Contracts with third-party service providers that were entered into prior to March 1, 2010 will satisfy the OCABR regulation if they are amended by March 1, 2012 to require vendors to implement and maintain appropriate security measures.

In FAQs promulgated in November 2009, the OCABR made the encryption requirement flexible. Consistent with the risk-based approach of the Massachusetts Regulation, the encryption requirement is technology-neutral in that it does not require specific encryption technology. Further, encryption is required only to the extent “technically feasible.” The phrase “technically feasible” is defined in the FAQs to mean “if there is a reasonable means through technology to accomplish a required result, then that reasonable means must be used.” The FAQs also note that backup tapes created on or after March 1, 2010 must be encrypted to the extent technically feasible, and existing backup tapes must also be encrypted if they are transported from current storage.

The FAQs also clarify other important issues, including the following:

- A bank or credit card account is a “financial account” which, when accompanied with the name of a Massachusetts resident, is subject to the Massachusetts Regulation. An account that is not clearly a financial account is considered a financial account if unauthorized access could result in an increase of financial burden or a misappropriation of monies, credit or other assets.

EDWARDS WILDMAN PALMER LLP

- An insurance policy number is a financial account number if it (i) grants access to a person's finances, or (ii) could result in an increase of financial burden, or a misappropriation of monies, credit or other assets.
- Compliance with HIPAA does not eliminate a company's obligation to comply with the Massachusetts Regulation if the company owns or licenses Personal Information of a Massachusetts resident.
- Businesses that only use credit card swipe technology and do not have actual custody or control over any Personal Information of a Massachusetts resident (as respects credit card transactions or employees) are not subject to the Massachusetts Regulation.
- Attorneys who own or license Personal Information must also comply with the Massachusetts Regulation, regardless of the protections offered by attorney-client privilege.

Companies, especially small businesses, that are subject to the Massachusetts Regulation have voiced concerns about the burden and costs of compliance. Although the OCABR amended the Massachusetts Regulation in response to some of those concerns, the OCABR has taken the position that the importance of protecting residents' Personal Information outweighs the financial burden on even small businesses that may need to retain outside consultants to help them institute the required procedures.

Recently, the Massachusetts Attorney General's Office commenced a significant enforcement action, signaling it would be taking a hard-line approach to enforcement of its consumer protection and privacy and data security requirements. In March 2011, it announced that the Briar Group, LLC, the owner of a group of popular restaurants in Massachusetts and elsewhere, agreed to pay a \$110,000 fine to the Attorney General's Office in connection with a data breach that allegedly affected over 125,000 credit and debit cardholders.¹²⁵ The AG's complaint did not allege violations of the Massachusetts Regulation or the Commonwealth's data breach statute, which were not yet in effect at the time of the breach. Rather, it alleged violation of Chapter 93A, the Massachusetts consumer protection statute. The AG complaint focused on the reported fact that a forensics investigator was not engaged until three weeks after the restaurant was informed of a potential breach (by credit card processors), and that the restaurant continued to accept credit and debit cards for several weeks after it allegedly knew or had reason to know that its security had been breached and thus that the cards of its customers continued to be vulnerable to theft. The complaint also alleged that the restaurant had failed to comply with Payment Card Industry Data Security Standards (PCI-DSS) and that it did not have other necessary data

¹²⁵ See Edwards Wildman Palmer LLP, *Massachusetts Attorney General Breaking New Ground in Data Security Enforcement?*, April 2011; Jenn Abelson, *Privacy Breach Case is Settled, Restaurant Group to Pay Mass. \$110,000*, March 29, 2011.

security precautions in place to protect its customer data. The Massachusetts AG took the position that these purported failures, notably including the lack of PCI-DSS compliance, contributed to the breach. This case may be an indication of the aggressive approach the Massachusetts AG will likely take going forward in enforcing Massachusetts privacy laws and regulations, and the scrutiny it will place on whether an entity that sustains a breach involving credit or debit cards complied with PCI-DSS security requirements as well as on the breached entity's reaction time.

2. Federal Requirements

In addition to state laws and regulations, entities may also be subject to federal rules and regulations mandating protection of Personal Information and requiring that certain steps be taken in the event of a data breach. Financial institutions in particular are subject to such federal regulations, and for these purposes, the term "financial institutions" is defined very broadly. Public companies may also need to disclose cyber risks and incidents as part of their mandated disclosure of material information to potential investors

a. Gramm-Leach-Bliley Act – Privacy and Safeguard Rules

The Gramm-Leach-Bliley Act ("GLBA") was enacted in 1999 to reform the financial services industry and address concerns relating to consumer financial privacy. Title V of the GLBA establishes a minimum federal standard of privacy and applies to financial institutions, including companies that were not traditionally considered to be financial institutions, such as insurance companies.¹²⁶

GLBA requires that the FTC and other governmental agencies that regulate financial institutions implement regulations to effectuate GLBA goals and requirements. The FTC issued the Privacy Rule and the Safeguards Rule under GLBA, both codified at 15 U.S.C. § 6801-6809. These Rules apply to insurance companies and other companies providing financial products to consumers.

The GLBA Privacy Rule requires these institutions to notify their customers when their information is shared with other parties. Customers have the right to "opt out" of intentional sharing of information if they do not want their financial institution to share their information with unaffiliated third parties.

The GLBA Safeguards Rule requires companies to develop a written information security plan that describes how they will protect customer information. The plan must be tailored to fit the company's size and complexity, the nature and scope of its activities, and the sensitivity of the customer information it handles.

¹²⁶ See <http://www.ftc.gov/privacy/privacyinitiatives/glbact.html> on the applicability of Title V of GLBA to insurance companies.

The five member agencies of the Federal Financial Institutions Examination Council -- the Federal Reserve Board, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of Currency, and Office of Thrift Supervision -- jointly issued “Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice” dated March 30, 2005 (“Guidance”), which interprets section 501(b) of GLBA and interagency security standards directed at ensuring the security and confidentiality of customer information, and implementing a response program in the event of unauthorized access. Among the minimum requirements of a response program, the Guidance requires timely notification of the entity’s primary federal regulator as soon as possible when an institution becomes aware of an incident involving unauthorized access to or use of “sensitive customer information,” and timely notification of customers as soon as possible after the institution determines that misuse of its information about a customer “has occurred or is reasonably possible.” The Guidance defines “sensitive customer information” as a customer’s name, address or telephone number in conjunction with the customer’s Social Security number, driver’s license, account number, credit or debit card number, or a personal identification number or password that would permit access to a customer’s account. It is also defined to include any combination of components of customer information that would allow someone to log onto or access the customer’s account, such as user name and password, or password and account number.

Thus, the GLBA imposes potentially applicable legal requirements both for instituting a security plan pre-breach and for providing notice of a data breach involving unauthorized access of Personal Information should one occur.

b. Federal Trade Commission “Red Flags” Rule

The FTC and other federal agencies that regulate financial institutions, including the Federal Reserve Board, National Credit Union Administration, Office of the Comptroller of Currency and Securities and Exchange Commission, have issued regulations to implement sections 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003 (“FACTA”).¹²⁷

FACTA is federal legislation directed at protecting consumers against identity theft as well as enhancing the accuracy of consumer report information. It prohibits businesses from printing out more than five digits of a credit card number, and allows consumers to obtain a free credit report every 12 months from each of the nationwide credit reporting agencies.

The new regulations, which are commonly referred to as the Red Flags Rule (the “Rule”),¹²⁸ are directed at preventing identity theft by requiring covered entities to develop and implement a written Identity Theft Prevention Program to detect the warning signs – the “red flags” – of identify theft in order to prevent and mitigate identity theft. The Rule applies to “financial

¹²⁷ Pub. Law 108-59, codified at 15 U.S.C. § 1681 *et seq.*

¹²⁸ 16 C.F.R. § 681.

institutions” and “creditors” that maintain “covered accounts,” as those terms are defined by the Rule. Although the Rule had been in effect since January 1, 2008 and traditional financial institutions regulated by the federal financial institutions regulatory agencies (such as banks) were required to comply by November 28, 2008, the FTC’s enforcement of the Rule, which was extended a number of times, became effective December 31, 2010 with regard to entities not previously under its scope.

(i) Affected “Financial Institutions” and “Creditors”

The Rule applies to “financial institutions” and “creditors” that maintain “covered accounts,” as those terms are defined by the Rule. “Financial institution” is defined as “a State or National bank, a State or Federal savings and loan association, a mutual savings bank, a State or Federal credit union, or any other person that, directly or indirectly, holds a transaction account ... belonging to a consumer.”¹²⁹

As initially enacted, the Rule’s definition of the term “creditor” was very broad, causing concern that the Rule would extend to entities other than traditional financial institutions that engage in regular forbearance in the collection of debts or bills or permit multiple or extended payments. On December 18, 2010, President Obama signed the Red Flag Program Clarification Act of 2010 into law, amending the Fair Credit Reporting Act’s definition of the term “creditor” to narrow the scope of the Rule. The revised definition of “creditor” specifically excludes those who advance funds on behalf of a person for expenses incidental to a service provided by the creditor to that person. As a result, many professionals who had challenged the scope of the Rule, including lawyers, accountants and healthcare professionals, are no longer subject to its requirements.

The Rule now defines “creditor” as used in the Rule as follows:

- (A) means a creditor, as defined in section 702 of the Equal Credit Opportunity Act¹³⁰ (15 U.S.C. § 1691a), that regularly and in the ordinary course of business
 - (i) obtains or uses consumer reports, directly or indirectly, in connection with a credit transaction;
 - (ii) furnishes information to consumer reporting agencies, as described in section 623, in connection with a credit transaction; or

¹²⁹ 15 U.S.C. § 1681a(t).

¹³⁰ “Any person who regularly extends, renews, or continues credit; any person who regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who participates in the decision to extend, renew, or continue credit.” 15 U.S.C. § 1691a.

- (iii) advances funds to or on behalf of a person, based on an obligation of the person to repay the funds or repayable from specific property pledged by or on behalf of the person;
- (B) does not include a creditor described in subparagraph (A)(iii) that advances funds on behalf of a person for expenses incidental to a service provided by the creditor to that person; and
- (C) includes any other type of creditor that the agency having authority over that creditor may determine appropriate by rule promulgated by that agency, based on a determination that such creditor offers or maintains accounts that are subject to a reasonably foreseeable risk of identity theft.”¹³¹

The December 18, 2010 amendment limited the definition of a creditor to cover only creditors who regularly, and in the ordinary course of business, carry out the following functions:

- Obtain or use consumer reports in connection with a credit transaction;
- Furnish information to consumer reporting agencies in connection with a credit transaction; or
- Advance funds to -- or on behalf of -- someone, except for funds for expenses incidental to a service provided by the creditor to that person.¹³²

(1) Covered Accounts

Significantly, the definition of “covered accounts” under the Red Flags Rule is also broad. It has two parts:

- (i) An account that a financial institution or creditor offers or maintains, primarily for personal, family or household purposes, that involves or is designed to permit multiple payments or transactions, such as a credit card account, mortgage loan, automobile loan, margin account, cell phone account, utility account, checking account, or savings account; and
- (ii) Any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and

¹³¹ 15 U.S.C. § 1681m(e).

¹³² See also <http://www.ftc.gov/bcp/edu/microsites/redflagsrule/index.shtml>.

soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks.¹³³

The second part of this definition extends the scope to any account for which there is a foreseeable risk of identity theft.

The Rule is designed to be risk-based and to take into account the burden that the Red Flags Rule could impose upon an entity that has only a small risk of identity theft. The FTC makes clear that higher-risk entities should have a more comprehensive Identity Theft Prevention Program, and low-risk entities are permitted to have a less complex program, but all entities covered by the Rule are required to establish a program.

In recognition of the burden that compliance with the Red Flags Rule may impose on certain entities, the FTC released a “Do-It-Yourself” Red Flag program for entities that are at low risk for identify theft.¹³⁴

(ii) Federal Information Security Management Act of 2002

The Federal Information Security Management Act of 2002 (“FISMA,” 44 U.S.C. § 3541, *et seq.*) is a United States federal law enacted as Title III of the E-Government Act of 2002, an act focused on the importance of information security to the economic and national security interests of the United States. FISMA requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.¹³⁵

(iii) Securities and Exchange Commission Guidance and Enforcement

(1) SEC Guidance Regarding Public Company Obligations to Disclose Cyber Security Risks and Incidents to Investors

Public companies need to assess their exposure to cyber risks and the procedures they take and costs they incur in preventing cyber incidents as part of their overall assessment of matters that can have a material effect on their company’s operations or financial condition.

On October 13, 2011 the Division of Corporation Finance of the Securities and Exchange Commission (SEC) issued guidance that identifies cyber risks and incidents as potential material information to be disclosed under existing securities law disclosure requirements and accounting

¹³³ 16 C.F.R. § 681.2(3).

¹³⁴ Available at <http://www.ftc.gov/bcp/edu/microsites/redflagsrule/get-started.shtm>.

¹³⁵ <http://csrc.nist.gov/groups/SMA/fisma/overview.html>.

standards (the “Disclosure Guidance”).¹³⁶ While the Disclosure Guidance states that it represents the views of the Division of Corporation Finance and is “not a rule, regulation or statement of the Securities and Exchange Commission,” public companies can now expect the SEC to review their filings to see whether cyber risks and incidents are adequately disclosed.

Federal regulations and guidance issued by other agencies in recent years have largely focused on identifying data security risks that would affect consumers. This Disclosure Guidance, however, is directed at protecting investors and encouraging companies to assess their risks of cyber incidents and review the adequacy of their disclosures as to those risks and their impact on a company’s operations, liquidity and financial condition. A broad range of factors are identified in the Disclosure Guidance for consideration, including prior cyber incidents, business operations and outsourced functions that have material cyber risks and potential costs and consequences, and relevant insurance coverage purchased by the company to address its exposures. Public companies now have a blueprint for assessing their cyber risk exposures, and for determining their reporting obligations as to material exposures, along with the context for evaluating such disclosures.

The Disclosure Guidance follows in the wake of a May 11, 2011 letter to the SEC from five members of the Senate, including John D. Rockefeller IV, Chairman of the U.S. Senate Committee on Commerce, Science, and Transportation. That letter expressed concern that “a substantial number of companies do not report their information security risk to investors,” and that “once a material network breach has occurred, leaders of publicly traded companies may not fully understand their affirmative obligation to disclose information” As a result, the Senators requested that the SEC “publish interpretative guidance clarifying existing disclosure requirements pertaining to information security risk”

The Disclosure Guidance was drafted to assist companies preparing disclosures required under U.S. federal securities laws (such as registration statements under the Securities Act of 1933 and periodic reports under the Securities Exchange Act of 1934) to assess whether they have a cyber risk exposure that should be disclosed.

(2) New SEC Enforcement of Data Security Requirements

In April 2011, the SEC announced that it had, for the first time, assessed financial penalties against individuals charged solely with violations of Regulation S-P, an SEC rule that requires financial firms to protect confidential customer information from unauthorized release to unaffiliated third parties.¹³⁷ According to the SEC, the fine was assessed pursuant to an SEC

¹³⁶ Securities and Exchange Commission, Division of Corporation Finance, CF Disclosure Guidance: Topic No. 2, Cybersecurity, October 13, 2011, available at <http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm>. See also, *Edwards Wildman Palmer Client Advisory*, Public Companies May Need to Disclose their Exposure to Material Cyber Risks According to New Guidance Issued by SEC Division of Corporation Finance, available at <http://www.edwardswildman.com/newsstand/detail.aspx?news=2634>.

¹³⁷ The SEC press release is available at: <http://www.sec.gov/news/press/2011/2011-86.htm>.

investigation that found that while a broker-dealer was winding down its business operations in 2010, its former president and former national sales manager violated customer privacy rules by improperly transferring customer records to another firm. The SEC also found that the former chief compliance officer failed to ensure that the firm's policies and procedures were reasonably designed to safeguard confidential customer information.

(iv) HIPAA Privacy and Security Rules

The U.S. Department of Health and Human Services ("HHS") has issued Standards for Privacy of Individually Identifiable Health Information (the "Privacy Rule") under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").¹³⁸

The Privacy Rule governs the use and disclosure of an individual's personal health information ("PHI") by entities covered under HIPAA. The Privacy Rule also sets standards for an individual's right to understand and control how his or her PHI is used. It applies to health plans, healthcare clearinghouses, and to any healthcare provider who engages in electronic data interchange using one or more of the "standard transactions" as defined by HIPAA (collectively referred to as "covered entities"). The Privacy Rule includes a requirement that a covered entity mitigate, to the extent practicable, any harmful effect that is caused by an improper disclosure of PHI of which it becomes aware. Under the HITECH Act, discussed below, the Privacy Rule also applies directly to business associates of covered entities.

A second major component of HIPAA is the Security Rule, which is directed at PHI in electronic form. The Security Rule sets forth required security standards for protecting electronically stored and transmitted PHI, including administrative safeguards (written procedures and protocols), physical safeguards (limitations on physical access to hardware, media, and software containing PHI), and technical safeguards (protective controls for information systems and networks). The HITECH Act also applied the Security Rule to business associates.

Importantly, the HITECH Act greatly increased the civil monetary penalties that could be imposed on covered entities and business associates for violations of the Privacy Rule or the Security Rule. It also vested limited enforcement power in state Attorneys General to enforce HIPAA's requirements.

As discussed below, the HITECH Act and the rules promulgated under it create additional requirements regarding notification to individuals of a data breach involving health information applicable to HIPAA covered entities or business associates of HIPAA covered entities.

¹³⁸ 42 U.S.C. § 201 *et seq.* (HIPAA), 45 C.F.R. Part 160 and Subparts A and E of Part 164 (Privacy Rule).

(v) The HITECH Act and Health Data Breach Notification Rules

The Health Information Technology for Economic and Clinical Health Act (the “HITECH Act”) under Title XIII of the American Recovery and Reinvestment Act of 2009, Public Law 111-5, also known as the Economic Stimulus Plan, directed the FTC and HHS to issue regulations with respect to data breaches involving personal health information.

Specifically, the FTC was directed to promulgate regulations requiring vendors of personal health records (“PHR”) and related entities to notify consumers when the security of their health information has been breached, and HHS was directed to promulgate a rule requiring (i) HIPAA covered entities, such as hospitals, doctors’ offices, and health insurance plans, to notify individuals of a security breach and (ii) business associates of HIPAA covered entities to notify such HIPAA covered entities in the event of a security breach.

(1) FTC Health Breach Notification Rule

The FTC’s final Health Breach Notification Rule (16 C.F.R. Part 318),¹³⁹ released on August 18, 2009, applies to a different group of entities than HIPAA. It applies to foreign and domestic vendors of PHR, PHR related entities and third-party service providers that maintain the information of U.S. citizens or residents. (The FTC Health Breach Notification Rule does not apply to HIPAA covered entities or any other entity that engages in activities as a business associate of a HIPAA covered entity. These entities are covered by the separate interim final rules issued by HHS on August 19, 2009, discussed below.)

The HITECH Act recognizes the new types of Web-based entities that collect consumers’ health information, such as vendors of PHR and Internet applications that interact with PHR. A PHR related entity means an entity, other than a HIPAA covered entity or any entity to the extent that it engages in activities as a business associate of a HIPAA covered entity, that:

- (1) Offers products or services through the website of a vendor of PHR;
- (2) Offers products or services through the websites of HIPAA covered entities that offer individual PHRs; or
- (3) Accesses information in a PHR or sends information to a PHR.

PHR related entities include, for example, web-based applications that help consumers manage medications and websites offering online personalized health checklists.

Under the FTC Health Breach Notification Rule, PHR vendors, PHR related entities and third-party service providers that experience a breach in the security of unsecured PHR identifiable health information must notify (i) individuals whose information was breached and (ii) the FTC.

¹³⁹ Set forth in the Federal Register, available at <http://www.ftc.gov/healthbreach/>.

PHR in this context means “an electronic record of PHR identifiable health information that can be drawn from multiple sources and that is managed, shared and controlled by or primarily for the individual.” “Breach of security” means acquisition of unsecured PHR identifiable health information of an individual in a PHR without authorization of the individual. “Unsecured” means PHR identifiable information is that not protected through the use of a technology as recommended by HHS in its guidance discussed below, that renders PHR identifiable health information unusable, unreadable, or indecipherable to unauthorized individuals.¹⁴⁰

Notice must be provided pursuant to the following requirements:

- **Timeliness of Notice:** Notice must be provided without reasonable delay and in no case later than 60 calendar days after the discovery of the breach of security. If the breach involves the unsecured PHR identifiable health information of 500 or more individuals, notice to the FTC must be provided no later than 10 business days after the date of discovery. If the breach involves fewer than 500 individuals, the entity may maintain a log of the breach and must submit it annually to the FTC no later than 60 calendar days following the end of the calendar year.
- **Method of Notice:** Notice to an individual affected by the breach may be sent in any of the following ways:
 - First-class mail to the individual’s last known address;
 - Email if the individual did not choose to receive first-class mail; or
 - Substitute notice, if the contact information for 10 or more individuals is insufficient or outdated, by conspicuous posting on the home page of the entity’s website for a period of 90 days or in major print or broadcast media, including in the areas where the affected individuals likely reside. The notice must include a toll-free phone number, which must remain active for at least 90 days, that individuals can call to learn whether they are affected by the breach.
- **Media Notice:** If 500 or more residents of a state or jurisdiction are, or are reasonably believed to be, affected by the breach, the entity must provide notice to prominent media outlets in the state or jurisdiction.
- **Content of Notice:** The notice must contain the following:

¹⁴⁰ 16 C.F.R. § 318.2.

- A brief description of what happened, including the date of the breach and the date of discovery of the breach, if known;
- A description of the types of unsecured PHR identifiable health information involved in the breach;
- Steps that individuals should take to protect themselves from potential harm resulting from the breach;
- A brief description of what the entity is doing to investigate the breach, mitigate harm, and protect against future breaches; and
- Contact information for individuals to ask questions or obtain additional information, including a toll-free number, email address, website, or postal address.

The FTC has issued a standard form to make it easier for companies to report a breach to the FTC.¹⁴¹

The FTC Health Breach Notification Rule was effective September 24, 2009, and the FTC began enforcing the data breach rules applicable to personal health record vendors and their contractors on February 22, 2010.

(2) The HHS Breach Notification Rule for HIPAA Covered Entities and Business Associates

HHS issued an interim final rule on the Breach Notification for Unsecured Protected Health Information for HIPAA covered entities and business associates of those entities, effective September 23, 2009 (the “HHS Rule”).¹⁴² Under the HHS Rule, covered entities must notify individuals whose unsecured protected health information (“PHI”) has been, or is reasonably believed to have been, accessed, acquired, used or disclosed following a breach of that unsecured PHI. Covered entities must also notify the media and HHS. The HHS Rule also requires that business associates notify the HIPAA covered entity of the breach.

The HHS Rule is similar to the FTC Health Breach Notification Rule. Its provisions regarding timeliness of notification, method of notification, and notice to the media are identical to those of the FTC rule. There are several important differences, however, including the following:

- Instead of notifying the FTC, the HHS rule requires covered entities to notify the Secretary of HHS;

¹⁴¹ The form is also available at <http://www.ftc.gov/healthbreach/>.

¹⁴² 74 Fed. Reg. 162 (August 24, 2009).

EDWARDS WILDMAN PALMER LLP

- Notices are required to be in plain language;
- If the breach affects more than 500 individuals of a particular state or jurisdiction, notice must be made to HHS contemporaneously with the notification to affected individuals; and
- In any case deemed by the covered entity to require urgency because of possible imminent misuse of unsecured PHI, the covered entity may provide information to individuals by telephone or other appropriate means in addition to written notice.

Full enforcement of the HIPAA data breach notification rule for covered entities began on February 22, 2010. In mid-February 2010, Adam H. Greene of the Office of General Counsel of the HHS Office for Civil Rights (“OCR”), which enforces the HIPAA rules, stated that enforcement of the business associate provisions would be delayed until final regulations are issued. OCR did not formally published notice of the enforcement delay.

On July 8, 2010, HHS issued a notice of proposed rulemaking to modify the HIPAA rules in accordance with the HITECH Act. The proposed rule was published in the Federal Register on July 14, 2010, and comments were accepted by HHS until September 13, 2010. HHS stated that it would allow covered entities and business associates a 180-day period after effectiveness of the final rule to come into compliance with “most of the rule’s provisions.” Among the changes was a proposal to expand the definition of “business associate” to include subcontractors of business associates which, if adopted, would make the HIPAA rules applicable to a much broader category of entities.

On July 28, 2010, to the surprise of many, HHS issued a statement withdrawing the proposed final version of the HHS Rule from review “to allow for further consideration” and noting that it is committed to ensuring that PHI is protected against unauthorized uses and disclosures. A new proposed final rule is expected to be published in the Federal Register eventually. Although the proposed final rule was withdrawn from consideration, the interim HHS Rule remains in effect. Consequently, covered entities must still notify HHS of data breaches.

In tandem with the HHS Rule, HHS also revised in important aspects a related document initially issued on April 17, 2009, called *Guidance Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals for the Purposes of the Breach Notification Requirements under the HITECH Act* (the “Guidance”).¹⁴³ HHS has clarified that covered entities and business associates are not required to follow the Guidance. If HIPAA covered entities and business associates, however, secure PHI in accordance with the Guidance, the PHI is deemed to be secure and thus a breach of the secured PHI would not be not subject to the notification requirements. The Guidance does

¹⁴³ 45 C.F.R. Parts 160 and 154.

not impose any obligation on covered entities to encrypt all PHI, but lists encryption as one of the two ways in which PHI may be rendered unusable, unreadable or indecipherable. The other method is destruction of the media on which the PHI is stored.¹⁴⁴

The push toward digitalization of medical records provided by the new legislation has raised concerns about a corresponding increase in risk of data breaches as medical information is increasingly maintained in electronic form. The increased risk is likely to result in further efforts to ensure compliance with the security requirements of the legislation.

Moreover, the issue of compliance with the privacy protection requirements of HIPAA and HITECH is also likely to be a component of third-party lawsuits against companies subject to the new rules that sustain data breaches. Lack of compliance with such regulatory safeguards is often a basis for claims of negligence in the security procedures of companies that sustain a breach.¹⁴⁵ Lack of compliance may also subject an entity to a suit brought by a state attorney general, as HITECH authorizes an attorney general to pursue an action against an entity that is subject to HIPAA when the attorney general “has reason to believe that an interest of one or more of the residents of [a] state has been or is threatened or adversely affected by any person who violates a [privacy or security provision under HIPAA].”¹⁴⁶

(vi) **Additional Data Privacy Requirements for Educational Institutions**

In the United States, any school or institution that provides educational services or instruction and receives funds under any program administered by the U.S. Department of Education is subject to the privacy requirements of the Family Educational Rights and Privacy Act (“FERPA”). Subject to certain limited exceptions, FERPA gives students (or in some cases their parents) the right to inspect and challenge the accuracy of a student’s own education records, while prohibiting schools from disclosing those records, or any personally identifiable information about a student contained in those records, without the student’s (or in some cases the parent’s) consent.

¹⁴⁴ Both the interim final HHS Rule and the Guidance are available at <http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveridentities/breachnotificationifr.html>.

¹⁴⁵ See *Amborg v. Express Scripts, Inc. et al.*, Civil Docket #4:09-VC-00705-FRB, filed in May 2009 in the U.S. District Court, Eastern District of Missouri. This lawsuit was commenced as a class action against an entity that provided pharmacy services and drug formulary management services to member groups including managed care organizations, insurance carriers and employer and union-sponsored health plans. It received an extortion demand by persons who had gained access to its customers’ confidential Personal Information. The plaintiffs based their complaint on, among other things, the company’s alleged failure to comply with HIPAA in a purported breach of assurances of compliance in its Privacy Notice.

¹⁴⁶ 42 U.S.C. § 1320d-5(d).

(vii) On the Horizon

There has been increasing recognition on the federal level of the growing risk of cyber attacks and the resultant exposures and disruptions to business, government operations and individual's interests. Thus, in recent years, the White House and federal agencies have issued policy frameworks and initiatives, and members of Congress have issued proposed numerous bills, in an effort to address privacy, data security and cyber security issues and risks. .

(1) Federal Privacy Frameworks

In December 2010, the Federal Trade Commission and the Department of Commerce both unveiled privacy frameworks outlining policy recommendations, which are expected to be influential in shaping forthcoming legislation.

(a) Federal Trade Commission

The FTC's preliminary staff report entitled *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers*¹⁴⁷ proposes a normative framework for how companies should protect consumers' privacy, and is intended to inform policymakers as they develop solutions, policies and potential laws governing privacy. The report is also intended to guide and motivate industry as it develops more robust and effective best practices and self-regulatory guidelines.

The proposed framework would apply broadly to online and offline commercial entities that collect, maintain, share, or otherwise use consumer data that can be reasonably linked to a specific consumer, computer or device. Among the guidelines outlined for companies in the proposed framework are: (i) building privacy protection into everyday business practices; (ii) providing choices to consumers about their data practices in a simpler, more streamlined way and providing a "Do Not Track" option; (iii) making data practices more transparent to consumers; (iv) providing consumers with reasonable access to the data that companies maintain about them; and (v) undertaking a broad effort to educate consumers about commercial data practices and the choices available to them.

The comment period ended on February 18, 2011, and the FTC reportedly received 452 separate comments regarding the proposed framework, which it is considering in its effort to issue a final report.¹⁴⁸

¹⁴⁷ Available at <http://www.ftc.gov/opa/2010/12/privacyreport.shtm>.

¹⁴⁸ Available at <http://www.ftc.gov/os/comments/privacyreportframework/index.shtm>.

(b) U.S. Department of Commerce

The U.S. Department of Commerce Internet Policy Task Force recently unveiled a green paper entitled *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework* (the “Green Paper”).¹⁴⁹ The Green Paper details initial policy recommendations aimed at promoting consumer privacy online while ensuring that the Internet remains a platform that spurs innovation, job creation, and economic growth. Key recommendations set forth in the Green Paper include: (i) consider establishing fair information practice principles comparable to a “Privacy Bill of Rights” for online consumers; (ii) consider developing enforceable privacy codes of conduct in specific sectors with stakeholders; (iii) create a privacy policy office in the Department of Commerce; (iv) encourage global interoperability to spur innovation and trade; (v) consider how to harmonize disparate security breach notification rules; and (vi) review the Electronic Communications Privacy Act for the cloud computing environment.

The Internet Policy Task Force has indicated that it will consider publishing a refined set of policy recommendations in the future.¹⁵⁰

(2) Proposed Federal Privacy, Data Security and Cyber Security Legislation

In recent years, numerous federal bills have been proposed with the goals of increasing consumer privacy and data security, combating breaches and theft from company and government computer networks, and imposing national breach notification requirements. There are currently a number of such bills pending before Congress. Washington policy makers and Congress finally seem poised to enact legislation in this area.

The focus of the currently pending bills and the current White House legislative proposal (also referred to as the Obama proposal) varies, but most would impose information security program requirements upon certain types of entities, particularly those in the industrial and public sectors, and many would replace state data breach notification requirements with federal requirements. Summaries of certain more significant bills currently under consideration, as well as the Obama proposal, are provided below.

In an indication of the increasing attention that data and cyber security risks are generating from federal policy-makers, there were a number of bills on the subject introduced in 2011 alone, with more expected.

On December 1, 2011, the House Intelligence Committee passed a cyber security data-sharing bill after making changes aimed at addressing privacy concerns raised by the White House and

¹⁴⁹ Available at <http://www.commerce.gov/node/12471>.

¹⁵⁰ See press release, available at <http://www.commerce.gov/news/press-releases/2010/12/16/commerce-department-unveils-policy-framework-protecting-consumer-priv>.

civil liberties groups, entitled The Cyber Intelligence Sharing and Protection Act of 2011. Its goal is reportedly to encourage the private sector and government to exchange information that could be useful in protecting systems critical to U.S. security and economic interests, including information detected in hacking incidents such as IP addresses and samples of malware.¹⁵¹

On May 12, 2011, the White House unveiled a comprehensive legislative proposal¹⁵² for increased cyber security measures and standardization of notification of breach obligations. The Administration's proposal includes provisions for: (i) creating a national notification standard; (ii) synchronization of penalties for computer crime with other types of crime, including mandatory minimum penalties for cyber intrusions into critical infrastructure, enabling the Department of Homeland Security to help and collaborate with private sector entities in responding to a cyber intrusion; (iii) voluntary sharing of information of new cyber threats but with privacy oversight to ensure that such actions do not adversely affect civil liberties or individual privacy; and (iv) formalizing the Department of Homeland Security's role in managing cyber security and the Federal Information Security Management Act.

On April 12, 2011, Senators John Kerry (D-MA) and John McCain (R-AZ) proposed the Commercial Privacy Bill of Rights Act of 2011 (the "Kerry-McCain Bill"), which seeks to establish a baseline code of conduct for how personally identifiable information and information that can uniquely identify an individual or networked device are used, stored, and distributed. The Kerry-McCain Bill seeks to provide consumers with (i) "the right to security and accountability," by requiring that collectors of information implement security measures to protect the information they collect and maintain; (ii) "the right to notice, consent, access, and correction of information" through specific notice, opt-in, opt-out, and access requirements; and (iii) "the right to data minimization, constraints on distribution, and data integrity" by restricting the collection of unnecessary data and the amount of time that data is retained, and by imposing new data security requirements. The Kerry-McCain Bill would not create federal data breach notification requirements, and would not preempt state notification requirements. In addition, the Kerry-McCain Bill does not provide a private cause of action; rather, its provisions would be enforced by the Federal Trade Commission and state attorneys general.

On April 13, 2011, Representatives Cliff Stearns (R-FL) and Rick Boucher (D-VA) proposed a bill that is similar, but that would grant federal agencies exclusive authority over consumer privacy, pre-empting state data breach notification laws, and thus reducing the current dilemma faced by entities that sustain a breach that implicates numerous, and often varying, state notification laws.

¹⁵¹ See Ellen Nakashima, *Cybersecurity legislation advances in Congress*, www.washingtonpost.com, posted December 2, 2011.

¹⁵² See fact sheet issued by the White House, available at http://www.whitehouse.gov/sites/default/files/fact_sheet-administration_cybersecurity_legislative_proposal.pdf.

On February 17, 2011, Senators Lieberman, Collin and Carper reintroduced their 2010 bill entitled “Protecting Cyberspace as a National Asset” as S. 413, the “Cyber Security and Internet Freedom Act of 2011.” S. 413 would amend the Homeland Security Act of 2002 and other laws in order to “enhance the security and resiliency of the cyber and communications infrastructure of the United States.” S. 413 has received attention mainly for the powers it would grant to the Department of Homeland Security to protect critical infrastructures upon declaration by the President of a “cyberemergency.” In addition, S. 413 also contains provisions requiring improvements to the federal government’s information security, the recruitment of federal “cyber security personnel,” and the funding of research into secure versions of Internet protocols.

Significantly, Senate Majority Leader Harry Reid (D-Nev.) and Senate Minority Leader Mitch McConnell (R-Ky.) have recently committed to work together on a comprehensive cyber security bill, and it is this forthcoming bill that legislative analysts have predicted will be seriously considered.¹⁵³ The Reid-McConnell bill is expected to be comprehensive, addressing privacy, data security and cyber security issues and risks, and based largely upon the currently pending bills and the Obama Administration proposal.¹⁵⁴

(3) Initiatives of the Obama Administration

In addition to the legislative proposal discussed above, the Obama Administration also issued the privacy, data security and cyber security policies, proposals and initiatives discussed below.

(a) Cyberspace Policy Review

On February 9, 2009, President Obama directed a comprehensive review to assess U.S. policies and procedures for cyber security, with the goal of developing a strategic framework to ensure that U.S. cyberspace initiatives are integrated, resourced and coordinated appropriately, both within the government and in the private sector. Upon completion of the review, findings and recommendations were released in the Cyberspace Policy Review (the “Review”).

According to the Review, cyber security risks pose some of the most serious economic and national security challenges of the 21st century,¹⁵⁵ and the United States’ digital infrastructure has suffered intrusions that have included theft of intellectual property and sensitive military information.¹⁵⁶ The Review indicates that the U.S. has so far not kept pace with the threats to

¹⁵³ Letter from Senate Majority Leader Reid to Senate Minority Leader McConnell, November 16, 2011.

¹⁵⁴ See *Congressional Update – Cybersecurity Policy and Legislation Update – December 2011*, an Edwards Wildman Palmer advisory available at www.edwardswildman.com/newstand/detail.as0070?news=2721.

¹⁵⁵ Cyberspace Policy Review, p. iii.

¹⁵⁶ Cyberspace Policy Review, p. i.

cyber security, and stresses the importance of leadership by the White House and partnership with the private sector in securing cyberspace.¹⁵⁷

Among the list of recommendations in the Review's Near-Term Action Plan are: (i) preparation of an updated national strategy to secure the information and communications infrastructure; (ii) initiation of a national public awareness and education campaign to promote cyber security; and (iii) preparation of a cyber security incident response plan.¹⁵⁸

(b) Office of the Cyber Czar

On May 29, 2009, President Obama implemented one of the recommendations from the Review's Near-Term Action Plan when he announced the creation of the office of "cyber czar" – a national cyber security chief to oversee the security of the U.S. communications networks and electronic infrastructure. On December 22, 2009, President Obama appointed Howard Schmidt, a former eBay and Microsoft executive, as the first cyber czar. Mr. Schmidt's duties include the protection of U.S. capabilities in cyber warfare and protection of Pentagon and defense related computer networks, as well as assisting the National Economic Council and reporting directly to Deputy National Security Adviser for Homeland Security and Counterterrorism John O. Brennan.¹⁵⁹ The inclusion in Mr. Schmidt's responsibilities of economic issues indicates a concern about cyber security that goes beyond military and defense issues.

On January 7, 2011, Mr. Schmidt and U.S. Commerce Secretary Gary Locke announced plans to create a National Program Office to coordinate federal activities needed to implement the National Strategy for Trusted Identities in Cyberspace (the "NSTIC Initiative"), an Obama administration initiative aimed at establishing identity solutions and privacy-enhancing technologies that will make the online environment more secure and convenient for consumers, as further discussed below.

(c) National Strategy for Trusted Identities in Cyberspace

In accordance with the Review, the Obama Administration issued the National Strategy for Trusted Identities in Cyberspace¹⁶⁰ (the "NSTIC Initiative") on April 15, 2011. The NSTIC Initiative presents a strategy for the public and private sectors to collaborate to increase the security of online transactions.

¹⁵⁷ Cyberspace Policy Review, p. v. Relatedly, the director of the CIA's clandestine information technology office has reportedly stated that the U.S. faces a shortage of cybersecurity experts, estimating that the U.S. requires between 10,000 and 30,000 people who are highly skilled at cybersecurity to defend the nation from online attacks, but stating that only about 1,000 are currently available. Matthew J. Schwartz, *Cybersecurity Expert Shortage Puts U.S. At Risk*, INFORMATION WEEK, July 21, 2010.

¹⁵⁸ Cyberspace Policy Review, p. vi.

¹⁵⁹ Ellen Nakashima, *Obama to name Howard Schmidt as cybersecurity coordinator*, The Washington Post, December 22, 2009.

¹⁶⁰ Available at http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf.

The NSTIC Initiative sets forth goals and a loose framework for a voluntary “Identity Ecosystem” that would replace the numerous usernames and passwords that consumers maintain with a single identification credential, such as a smart card or a smart phone application. Guiding principles of the NSTIC Initiative are: (i) the enhancement of privacy and support of civil liberties; (ii) secure and resilient identity solutions; (iii) ensuring policy and technology interoperability among identity solutions; and (iv) that the Identity Ecosystem must be built from identity solutions that are cost-effective and easy to use.

The NSTIC Initiative contemplates primary development and implementation of the Identity Ecosystem by the private sector, although the Federal Government intends to coordinate private and public sector involvement and plans to implement the Identity Ecosystem for the services it provides internally and externally. According to the NSTIC Initiative, the Federal Government will neither mandate that individuals obtain an Identity Ecosystem credential nor that companies require Identity Ecosystem credentials from consumers as the only means to interact with them.

The Department of Commerce is in the process of developing the structure of a steering group that will administer policy and standards adoption for the Identity Ecosystem Framework. The Department of Commerce issued a Notice of Inquiry on June 8, 2011, seeking public comment on the formation and structure of the steering group. Comments were due August 30, 2011, and 57 separate public comments were submitted.

(d) Call for International Standards

On May 16, 2011, the White House released its first comprehensive International Strategy for Cyberspace¹⁶¹ (the “International Strategy”). The International Strategy is a policy document that “explains what the U.S. stands for internationally in cyberspace, and how it plans to build prosperity, enhance security, and safeguard openness in our increasingly networked world,” according to White House Cybersecurity Coordinator Howard Schmidt.¹⁶² The “action lines” of the International Strategy are aimed at achieving the following objectives: (i) promoting international economic standards and innovative, open markets; (ii) protecting our networks by enhancing security, reliability, and resiliency; (iii) law enforcement: extending collaboration and the rule of law; (iv) preparing for 21st Century military security challenges; (v) improving Internet governance by promoting effective and inclusive structures; (vi) international development: building capacity, security, and prosperity; and (vii) supporting fundamental freedoms and privacy on the Internet.

Of note, the International Strategy refers to potential use of military force in response to cyber attacks, stating:

¹⁶¹ Available at http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

¹⁶² See post to White House Blog, available at <http://www.whitehouse.gov/blog/2011/05/16/launching-us-international-strategy-cyberspace>.

When warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country. We reserve the right to use all necessary means – diplomatic, informational, military, and economic – as appropriate and consistent with applicable international law, in order to defend our Nation, our allies, our partners, and our interests.¹⁶³

According to media reports, UK Prime Minister David Cameron expressed agreement with this position in a November 1, 2011 speech at the London Conference on Cyberspace, stating that the UK would respond to cyber attacks “as robustly as any other national security threats.”¹⁶⁴

3. Industry Standards: PCI Standards for the Protection of Credit Card Information

The Payment Card Industry Security Standards Council is an international organization founded by American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc. in 2006 to develop and manage certain credit card industry standards, including the Payment Card Industry Data Security Standards (“PCI-DSS”).

PCI-DSS is a set of requirements created to help protect the security of electronic payment card transactions that include Personal Information of cardholders, and operate as an industry standard for security for organizations utilizing credit card information. PCI-DSS applies to all organizations that hold, process or pass credit card holder information. It imposes requirements upon those entities for security management, policies, procedures, network architecture, software design and other critical measures that help to protect customer credit and debit card account data. As a large number of malicious data breaches are targeted at obtaining electronically transmitted, collected or stored payment card information, PCI-DSS compliance is often one of the first aspects investigated when a breach occurs involving payment card information. The effectiveness of the PCI-DSS requirements for minimizing the risk of data breach is a subject of some debate; however, according to one study, 89% of companies suffering a data breach in 2010 that were subject to PCI-DSS had not achieved compliance.¹⁶⁵

Under PCI-DSS, merchants and service providers are categorized according to the number of credit card transactions they process in a 12-month period, and compliance obligations differ depending on such designations. For example, a Level 1 designation indicates that the merchant is among those with the largest number of transactions and the greatest level of security required. Level 1 merchants process more than six million credit card transactions annually, across all

¹⁶³ *Id.*

¹⁶⁴ UK Aligning with US Cyber War Response Strategy?, IT PRO, Nov. 1, 2011, available at <http://www.itpro.co.uk/637099/uk-aligning-with-us-cyber-war-response-strategy>.

¹⁶⁵ *2011 Data Breach Investigations Report*, A study conducted by the Verizon RISK Team in cooperation with the United States Secret Service and the Dutch High Tech Crime Unit.

channels, including the Internet, and must perform an on-site PCI data security assessment on an annual basis and network scans on a quarterly basis.

PCI-DSS provides for fines and penalties against organizations that fail to comply with PCI-DSS standards. These standards and the fines involved are essentially contractual private arrangements rather than government regulatory schemes, although government entities are starting to adopt these standards, as discussed below. When a data breach occurs involving credit card information maintained by an entity subject to PCI-DSS, and the breached entity has not satisfied PCI-DSS standards, the associated fines and penalties can be quite substantial. The deviation from PCI-DSS standards can be used as evidence of departure from industry standards in both industry investigations and third-party lawsuits.

The card brands may levy significant fines and penalties on merchants that are not in compliance with PCI-DSS. Such penalties and fines, imposed separately by each card association, can include:

- Hefty fines (in multiples of \$100,000) for prohibited data retention;
- Significant additional monthly fines (can be \$100,000 or more per month depending on the nature of the data stored) assessed until confirmation is provided indicating that prohibited data is no longer stored;
- Separate fines (in multiples of \$10,000) for PCI-DSS non-compliance;
- Additional monthly fines (likely \$25,000 per month) assessed until confirmation from a qualified security assessor that the merchant is PCI-DSS compliant;
- Payment of monitoring (can be as high as \$25) and reissuing (up to \$5) assessments for each card identified by the card association as potentially compromised; and
- Reimbursement for any and all fraudulent activity the card association identifies as being tied to a security data breach.

In addition, after a breach, a merchant's classification or tier will usually be adjusted upwards to Level 1, regardless of the number of credit card transactions it processes, resulting in the imposition of further obligations and potentially even greater fines and penalties should another breach occur. Merchants are responsible for all costs associated with any system modifications required to achieve PCI-DSS compliance.

a. Incorporation of PCI-DSS into State Law

Several states, such as Minnesota, Nevada and Washington, have incorporated PCI-DSS requirements into their data protection laws, as detailed below.

(i) Minnesota

The Minnesota Plastic Card Security Act,¹⁶⁶ enacted on May 21, 2007, is the first of its kind. This act prohibits companies that accept payment cards from retaining card security code data, PIN verification code numbers or the full contents of any track of magnetic stripe data after 48 hours following authorization of a transaction. If a company has violated the 48-hour rule, financial institutions may recover from the company if there has been a security breach exposing payment card data.

(ii) Nevada

A new amendment to Nevada data protection law that became effective January 1, 2010, requires companies doing business in Nevada that accept payment cards to comply with PCI-DSS.¹⁶⁷ The new amendment also requires that other data collectors doing business in Nevada encrypt personal information contained in certain kinds of transmissions and when stored on a data storage device.

(iii) Washington

Under a Washington law effective July 1, 2010, if a credit or debit card processor or business fails to take reasonable steps to guard against unauthorized access to account information that is in its possession, and such failure is found to be the proximate cause of a breach, the processor or business is liable to financial institutions such as banks that issued the credit cards for reimbursement of their reasonable actual costs related to the reissuance of credit or debit cards, even if the financial institution has not suffered another injury as a result of the breach.¹⁶⁸ The processor or business may also be liable to the financial institution for attorneys' fees and costs incurred in connection with any legal action. In addition, vendors of card processing software and equipment may be held liable for the damages incurred by a financial institution if the vendor's negligence was the proximate cause of such damages. The new law provides for several exemptions. Processors, businesses and vendors that are compliant with PCI-DSS at the time of the breach are not liable to financial institutions. They are considered to be compliant if their PCI data security compliance was validated by an annual assessment, and if the assessment took place no more than one year prior to the date of the breach. In addition, processors, businesses and vendors are not liable if the breach involved encrypted card information.

While Minnesota, Nevada and Washington appear to be the only states to incorporate PCI-DSS requirements in their data breach laws as of November 2011, other states may soon follow.

¹⁶⁶ Minn. Stat. § 325E.64.

¹⁶⁷ Nev. Rev. Stat. § 603A.215.

¹⁶⁸ Wash. Rev. Code § 19.255.

4. International

a. Introduction

Global compliance with data protection laws is likely to present an increasing challenge, as the number of jurisdictions with such laws, and the fines for their violation, increase.

Many companies' operations may be affected by the data security laws of multiple countries, apart from the jurisdiction in which they are domiciled. Many companies have subsidiaries, affiliates or employees in other countries. Thus, for example, a U.S. company that sustains a breach that includes Personal Information of international customers may need to consider carefully the impact of the data security and breach notification laws of other countries, and whether they impose reporting or notification obligations on the U.S. breached company.

In addition to the Member States of the European Union ("E.U."), over 45 other countries now have data protection or privacy laws and others are in the process of developing them. Some of those with existing laws are contemplating revising them to enhance obligations, and increase penalties for non-compliance.

Aspects of the E.U. Data Protection Directive, as well as selected countries' national laws and enforcement powers, are considered below.

b. The European Union

Many U.S. companies maintain subsidiaries, affiliates or employees in the E.U. Such companies, whether or not publicly traded, must comply with relevant E.U. Member States' data protection laws and guidelines where "personal data" (as defined by the pertinent law) is collected, processed or transferred by local operations.

(i) E.U. Data Protection Directive

E.U. Member States' data protection laws are based on E.U. Directive 95/46/EC, known as the "Data Protection Directive." The Data Protection Directive itself is not binding on individual natural or legal persons. Member States are required to implement the Data Protection Directive by passing national laws. There is considerable variation between Member States' interpretation and implementation of the Data Protection Directive, and thus individual Member States' laws must be considered as well as the Data Protection Directive.

Under the Data Protection Directive, responsibility for compliance rests with the "controller," who is the natural or legal person who alone or jointly with others determines the purposes and means of the processing of personal data. Subject to certain exceptions, controllers are required to notify their national data protection authority of their data processing activities.

The Data Protection Directive requires controllers to process personal data only in accordance with certain data protection principles, such as the requirements that data be processed fairly and

lawfully and that there be implementation of appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access.

Under the Data Protection Directive, the meaning of “personal data” is broader than the term “Personal Information” generally applicable in the U.S. (and broader than as used elsewhere in this paper). It includes any information relating to an identified or identifiable natural person.

Controllers are prohibited from transferring personal data to countries outside the E.U. that do not ensure an adequate level of protection of personal data. The U.S. is not currently considered to provide such an adequate level of protection¹⁶⁹ and thus personal data may not be transferred from the E.U. to persons in the U.S. without additional protections. Such additional protections include the transferee being enrolled in the Safe Harbor program,¹⁷⁰ under which the transferee voluntarily agrees to be bound by data protection rules broadly equivalent to those set out in the Data Protection Directive, or entering into a compliant data transfer agreement.

U.S. companies may encounter such a prohibition on transfer in a wide range of circumstances. For example, in a recent U.S. court case,¹⁷¹ a Utah court ordered a U.S. company to disclose customer complaint data that was relevant to a claim that had been filed against it, notwithstanding that the data was located in Germany and the transfer to the U.S. may breach German data protection laws. The court was not sympathetic to the dilemma faced by the U.S. company. One concern is that to allow other countries’ data transfer restrictions to trump U.S. court directions to produce information in U.S. legal proceedings could operate to encourage transfer of sensitive and perhaps unfavorable information outside the U.S. in jurisdictions that render transfer back into the U.S. difficult.

On April 20, 2010, the European Commission (the “Commission”), the executive body of the E.U., set out a plan¹⁷² for the implementation of the Stockholm Programme, a plan of E.U. justice and security policies for 2010 to 2014, which it adopted in December 2009. Among other things, the Commission plans to draft a new legal framework for data protection by modernizing the Data Protection Directive.¹⁷³

In April 2011, the Article 29 Working Party, an influential advisory body made up of representatives from the data protection authority (“DPA”) of each E.U. Member State, the

¹⁶⁹ Opinion 1/99 concerning the level of data protection in the United States and the ongoing discussions between the European Commission and the United States Government, EC Commission Working Party on the Protection of Individuals with regard to the Processing of Personal Data.

¹⁷⁰ Commission Decision 2000/520/EC of 26.7.2000.

¹⁷¹ *AccessData Corp. v. Alste Techn. Gmbh*, 2010 WL 318477 (D. Utah Jan. 21, 2010).

¹⁷² Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions of 20 April 2010 – Delivering an area of freedom, security and justice for Europe’s citizens – Action Plan Implementing the Stockholm Programme.

¹⁷³ *Id.*

European Data Protection Supervisor and the European Commission stated its support for the extension of data breach notification to cover all data controllers.¹⁷⁴

At the October 2011 plenary meeting of the Article 29 Working Group,¹⁷⁵ the Working Group announced that it planned to send its proposals for a mechanism to ensure cooperation and coordination between DPAs and consistent application of the Data Protection Directive to the European Commissioner for Justice, Fundamental Rights, and Citizenship.

On December 6, 2011, Viviane Reding, the Vice-President of the European Commission and E.U. Commissioner for Justice, Fundamental Rights and Citizenship, laid the foundation for a comprehensive reform of European data protection laws at the 2nd Annual European Data Protection and Privacy Conference in Brussels. At the same time, a draft of the European Commission's current proposal for the new General Data Protection Regulation, as it has been called, was leaked. While this is still subject to internal discussions, it provides an insight into the revised data protection landscape. The proposed reform will impact every business that operates in the E.U., including U.S. organizations targeting European business. This reform is expected to be formally announced in early 2012.¹⁷⁶

It is anticipated that the proposed Regulation will introduce a general requirement to notify DPAs and data subjects where there has been a data loss. In addition, data breaches would need to be notified to a DPA within 24 hours. While this has recently become a requirement for telecommunications and Internet service providers under an existing E.U. Directive,¹⁷⁷ the proposed Regulation extends this requirement to all organizations. Given the increase in global cyber risks and the reputational impact and associated costs of data losses and breaches, this aspect of the reform is likely to have a significant impact on businesses in the E.U.

(ii) Cookies and other tracking technologies

In November 2009, an amendment to the E.U. E-Privacy Directive¹⁷⁸ was adopted that required E.U. Member States to ensure that the storing of or access to information such as cookies, spyware or other tracking devices on the equipment of an Internet user is permitted only if the user has been provided with clear and comprehensive information about the purposes of the processing and has given his or her consent. Prior to this amendment, user consent was not required and users had only to be given the opportunity to refuse the storing of or access to devices (which was commonly achieved by the user adjusting browser settings to prevent such

¹⁷⁴ Working Document 01/2011 on the current E.U. personal data breach framework and recommendations for future policy developments.

¹⁷⁵ Press release of Article 29 Data Protection Working Party - 82nd meeting, 13-14 October 2011.

¹⁷⁶ See *Client Advisory- Companies Prepare for European Data Protection Reform*, an Edward Wildman Palmer Privacy & Data Protection Group Advisory, available at www.edwardswildman.com/newsstand/detail.aspx?news=2680.

¹⁷⁷ Directive (2009/136/EC) amending the Privacy and Electronic Communications Directive (2002/58/EC).

¹⁷⁸ *Id.*

storage or access). There is an exception to the requirement to obtain consent where the storage is strictly necessary for a service expressly requested by the user. E.U. Member States were required to pass national legislation implementing the amendment to the E-Privacy Directive by May 26, 2011. As of January 1, 2012, a number of E.U. Member States had not yet implemented the relevant amendments to the E-Privacy Directive and the European Commission had commenced legal action against these E.U. Member States for failure to implement.¹⁷⁹

The Article 29 Working Party has taken the position that the requirements for consent are for “prior consent” and that all information must be provided and consent obtained before any information is sent or collected from a user’s device.¹⁸⁰ This gives rise to complicated and prohibitive pop-ups or similar notifications for users, particularly where there are numerous third-party advertising networks involved. On the other hand, advertising networks, advertisers and content providers are seeking to rely on Recital 66 of the E.U. E-Privacy Directive, which seems to offer a more pragmatic approach to consent by inferring that prior consent is only required “where it is technically possible and effective.” In addition, Recital 66 also infers that consent may be obtained through the use of “appropriate settings of a browser or other application.” The Interactive Advertising Bureau (IAB) Europe and the European Advertising Standards Alliance (EASA) have sought to build on this pragmatic approach with industry-led solutions providing for a means of opting-out from tracking.¹⁸¹ However, the Article 29 Working Party has been repeatedly very critical of these solutions and this has raised issues as to whether they comply with law.¹⁸²

The UK DPA has issued guidance¹⁸³ that it will allow a 12-month grace period, ending in May 2012, for companies to develop ways of complying with the UK’s national legislation implementing the amendment to the E-Privacy Directive.

(iii) The Dilemma of Whistleblower Hotlines

Many multi-national companies have implemented whistleblower hotlines, which permit employees and service providers to report allegations of fraud, infractions of codes of conduct or similar complaints. For U.S. companies, such hotlines are often part of compliance with the Sarbanes-Oxley Act of 2002, the Foreign Corrupt Practices Act of 1977 or other U.S. laws.

Implementing such hotlines in E.U. Member States gives rise to certain data protection issues, which should be given careful consideration.¹⁸⁴ In some Member States, amendments must be

¹⁷⁹ Digital Agenda: Commission starts legal action against 20 Member States on late implementation of telecoms rules.

¹⁸⁰ Available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2011/20110803_letter_to_oba_annexes.pdf.

¹⁸¹ http://www.easa-alliance.org/News/News/page.aspx/46?xf_itemId=146&xf_catId=1.

¹⁸² http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp188_en.pdf.

¹⁸³ *Enforcing the revised Privacy and Electronic Communications Regulations (PECR)*, May 25, 2009.

made to the hotline reporting procedure in order to comply with local laws or guidelines. Certain issues which may arise in selected Member States are considered below. In February 2006, the Article 29 Working Party issued an opinion¹⁸⁵ to provide guidance to industry in establishing whistleblower hotlines throughout the E.U. that were compliant with both the Sarbanes-Oxley Act and the Data Protection Directive, although individual Member States' laws and guidance must still be considered.

Most E.U. Member States require notification of hotlines to the relevant DPA, and in some Member States hotlines cannot be operated until approval has been obtained. Where hotlines involve the transfer of personal data from the E.U. to the U.S., Member States will require certain contractual and technical security measures to be in place. Company works councils may need to be consulted prior to the implementation of a whistleblower hotline.

c. Selected Countries' Data Protection Laws

E.U. Member states have passed their own national data protection laws in order to implement the Data Protection Directive. Many non-E.U. countries have also instituted data protection laws in recent years, addressing what is a worldwide problem and presenting additional compliance issues for companies with multinational operations.

(i) United Kingdom ("UK")

In the UK, the Data Protection Directive was implemented by the Data Protection Act 1998 ("UK Act"). The Information Commissioner's Office ("ICO") is responsible for ensuring compliance with, and bringing enforcement action for breaches of, the UK Act.¹⁸⁶ Since April 6, 2010, the ICO has had the power to impose fines of up to £500,000 where there has been a serious contravention of the principles set out in the UK Act and certain other requirements are met. On December 6, 2011, the ICO fined Powys County Council £130,000, its largest fine so far. This was in connection with a serious breach of the UK Act, where the details of a child protection case were sent to the wrong recipient. As of December 31, 2011, the ICO had imposed nine fines for breaches of the UK Act.

In the UK, regulated financial services firms, such as banks and insurance companies and brokers, must also comply with the rules prescribed by the Financial Services Authority ("FSA"). The FSA's enforcement powers include private censure, removal of authorization, withdrawal of approved person status and potentially large fines. In July 2009,¹⁸⁷ the FSA fined

¹⁸⁴ See Schreiber, Mark, et al, *The Practitioner's Guide to The Sarbanes-Oxley Act*, Volume II, Chapter 9 – *Anonymous Sarbanes-Oxley Hotlines for Multi-National Companies: Compliance with EU Data Protection Laws*, 2009 and <http://www.ico.gov.uk/news/blog/2011/half-term-report-on-cookies-compliance.aspx>.

¹⁸⁵ Opinion 1/2006 on the application of EU data protection rules to internal whistleblowing schemes in the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime.

¹⁸⁶ More information about the UK Act and the ICO is available at www.ico.gov.uk.

¹⁸⁷ Available at: <http://www.fsa.gov.uk/Pages/Library/Communication/Notices/Final/2009/index.shtml>.

an insurer, insurance broker and actuarial consultancy in the HSBC Group a total of £3.19m for information security failings, including sending unencrypted customer details through the mail to third parties, leaving confidential information about customers in unlocked cabinets and not giving staff sufficient training on how to identify and manage risks like identity theft. More recently, in August 2010,¹⁸⁸ the FSA fined an insurer £2,275,000 for failing to have adequate systems and controls in place to prevent loss of customers' information. During a routine transfer to a data storage center, a subcontractor of an affiliate which provided processing services to the insurer lost an unencrypted back-up tape containing 46,000 customers' personal details, including identity details, and in some cases bank account and credit card information, details about insured assets and security arrangements. The FSA found that the insurer had failed to manage the risks relating to the security of confidential customer information arising out of the outsourcing arrangement.

(ii) Germany

In Germany, the Data Protection Directive was implemented by the Federal Data Protection Act 2001¹⁸⁹ ("German Act"). Germany has a number of regional DPAs rather than a single national DPA.

Under the German Act, a data controller must notify the relevant German DPAs and affected data subjects if it determines that certain serious or sensitive categories of personal data have been recorded, unlawfully transferred or otherwise unlawfully disclosed to third parties, threatening serious harm to the data subjects' rights or legitimate interests. If notifying all affected data subjects individually would require a disproportionate effort, notification can be replaced by public advertisements in daily newspapers or other effective means.

German DPAs have the power to impose fines of up to €50,000 for simple violations and €300,000 for serious violations of the German Act and to order organizations to remedy compliance failures.

In April 2007, a working group of German DPAs adopted a report entitled "Whistleblowing - Hotlines: Internal Warning Systems and Employee Data Protection"¹⁹⁰ that introduces guidelines to allow companies to introduce whistleblower hotlines which are compliant with German data protection law. A company's works council needs to be consulted prior to implementation of a whistleblower hotline and the works council has a right of co-determination, such that the terms of the hotline program are to be negotiated with them.

¹⁸⁸ Available at: <http://www.fsa.gov.uk/Pages/Library/Communication/Notices/Final/2010/index.shtml>.

¹⁸⁹ Federal Data Protection Act (Bundesdatenschutzgesetz), published in the Bundesgesetzblatt I Nr. 23/2001, page 904 on 22 May 2001.

¹⁹⁰ Available at: <http://fhh.hamburg.de/stadt/Aktuell/weitere-einrichtungen/datenschutzbeauftragter/informationmaterial/wirtschaft/whistleblowing.html>.

(iii) France

In France, the Data Protection Directive was implemented through an amendment to the existing law 78-17 of January 6, 1978 relating to the Protection of Data Subjects as Regards the Processing of Personal Data.¹⁹¹

In November 2005, the French DPA published guidelines¹⁹² to assist companies in the introduction of whistleblower programs that are compliant with both the Sarbanes-Oxley Act and French law. Since then, the French DPA has had a two-tier system of authorization in place, under which whistleblower programs may be authorized by either: (a) self-certifying to the French DPA through an automated on-line process that a whistleblower program complies with certain specified parameters (the “AU-004 authorization”); or (b) seeking the French DPA’s formal approval.

In July 2011, revised guidance¹⁹³ issued by the French DPA for the AU-004 authorization became mandatory, narrowing the permitted scope of whistleblower programs that qualify for AU-004 authorization. Companies wishing to qualify for the AU-004 authorization must now restrict their whistleblower program scope to concerns about accounting, financial, banking, anti-competitive or corruption matters. Matters in the “vital interests” of the company or its employees’ physical or mental integrity, which were permitted under the earlier guidance, are now outside the scope of whistleblower programs that qualify for AU-004 authorization. These other serious “vital interests” matters arguably covered matters relating to discrimination, environmental violations, violations of workplace safety rules and disclosures of trade secrets.

In April 2011, the French DPA announced that it intends to increase inspections of companies transferring data into and out of France to ensure compliance with French data protection laws.¹⁹⁴ The inspections will include a focus on verifying that U.S. companies enrolled in the Safe Harbor program are, in fact, compliant with its rules.

(iv) Spain

In Spain, the Data Protection Directive was implemented through Organic law 15/99 of December 13, 1999 on the Protection of Personal Data.

The Spanish DPA has issued an opinion to the effect that it considers anonymous reports to be unsuitable and not permissible for a whistleblower hotline in Spain. Notification to the Spanish DPA is required, so it has the opportunity to carry out a review of whistleblower programs and

¹⁹¹ Available at: www.cnil.fr/fileadmin/documents/en/Act78-17VA.pdf.

¹⁹² Available at: <http://www.cnil.fr/fileadmin/documents/en/CNIL-recommandations-whistleblowing-VA.pdf>.

¹⁹³ Available at: <http://www.cnil.fr/en-savoir-plus/deliberations/deliberation/delib/83/>.

¹⁹⁴ Available at: http://www.cnil.fr/la-cn/il/actu-cn/il/article/article/programme-des-controles-2011-une-ambition-reaffirmee-des-competences-elargies/?tx_ttnews%5bbackPid%5d=2&cHash=91ae300acd.

confirm compliance with local law. There may be options for compliance in Spain, outside the hotline system, for making reports but this area is still unsettled.

Under one of the data protection principles set out in the Data Protection Directive discussed above, controllers must process personal data fairly and lawfully (the “fair processing principle”). In most E.U. Member States, controllers may seek to comply with the fair processing principle on the basis that processing is for the purposes of legitimate interests pursued by the data controller (the “legitimate interests condition”). The legitimate interests condition gives controllers a broad basis on which to comply with the fair processing principle. Under Spanish law, the legitimate interests condition is not available to data controllers and so other, less flexible, conditions must be relied upon instead. As of late 2011, the European Court of Justice is expected to hear a case submitted by the Spanish Supreme Court as to whether Spain has failed to properly implement the Data Protection Directive by not making the legitimate interest condition available to controllers.

(v) Sweden

In Sweden, the Data Protection Directive was implemented through the Personal Data Act 1998¹⁹⁵ (“Swedish Act”).

Under the Swedish Act, it is generally prohibited for companies to process data relating to criminal allegations or violation of law, including in a hotline. Companies wishing to operate a hotline in Sweden must therefore apply to the Swedish DPA for an exemption from such prohibition. The Swedish DPA has a policy of granting such exemptions subject to certain restrictions, including that only key personnel and employees in a management position may be reported and personal data relating to other groups of employees may not be processed through the hotline. This may require certain language in the notice to employees in Sweden that the hotline should be used only where the report relates to a member of management or a key employee of the company. In some cases, it may not always be possible to impose such a limitation or the boundaries may become inevitably blurred.

(vi) Mexico

On April 27, 2010, the Mexican Senate passed a data protection law that addresses how private and public entities handle the collection, use and disclosure of personal information of Mexican residents.¹⁹⁶ The new law expands the authority of the Mexico’s data protection authority, now called the Federal Institute of Access to Information and Data Protection (“IFAI”). On October 21, 2011, the IFAI co-published a second draft of regulations implementing the new data protection law, inviting public comment.¹⁹⁷ The proposed regulations include provisions

¹⁹⁵ Available at: <http://www.regeringen.se/content/1/c6/01/55/42/b451922d.pdf>.

¹⁹⁶ Available at: <http://www.senado.gob.mx/index.php?ver=sp&mn=2&sm=2&id=2879&lg=61>.

¹⁹⁷ Available at: [http://www.cofemermir.gob.mx/uploadtests/24470.131.59.1.ANTEPROYECTO%20DEL%](http://www.cofemermir.gob.mx/uploadtests/24470.131.59.1.ANTEPROYECTO%20DEL%20)

dealing with data transfers and security and data breach notification. As of late 2011, the regulations were expected to be finalized shortly.

(vii) Canada

On May 1, 2010, Alberta became the first Canadian province to pass a general data breach notification law.¹⁹⁸ Bill 54 added new sections to The Personal Information Protection Act, requiring notice of a data breach to affected individuals and Alberta's Information and Privacy Commissioner. Notice to individuals is only required if there is a "real risk of significant harm."

(viii) India

In April 2011, India adopted new privacy regulations, known as the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 (the "Indian Rules").¹⁹⁹ The Indian Rules impose a number of obligations on data controllers, including: a requirement to have a privacy policy in place; a requirement to obtain the consent of data subjects prior to the collection or processing of sensitive personal data; restrictions on disclosure of personal data to third parties and the transfer of personal data overseas; and a requirement to comply with reasonable security practices and procedures.

Guidance issued by the Ministry of Communications and Information Technology clarifies that the Indian Rules will apply to Indian entities only and that several provisions, including those relating to the collection and disclosure of personal information, will not apply to Indian outsourcing services providers, other than in relation to the data of their own India-based personnel or customers, or to individuals who contract directly with them.²⁰⁰

(ix) China

In February 2011, the People's Republic of China's General Administration for Quality Supervision, Inspection, and Quarantine and the Commission for the Administration of Standardization circulated draft Information Security Technology Guidelines for Personal Information Protection (the "China Personal Data Guidelines").²⁰¹ If implemented, the China Personal Data Guidelines would be guidelines only and not enforceable at law.

The China Personal Data Guidelines include a set of principles relating to the collection, processing and use of personal data. These include the following: an individual should be notified as to the manner of collection, processing and disclosure of his or her personal information; personal information should generally only be used for the notified purposes; and

¹⁹⁸ Available at: http://www.qp.alberta.ca/570.cfm?frm_isbn=9780779748938&search_by=link.

¹⁹⁹ Available at: [www.mit.gov.in/sites/upload_files/dit/files/GSR313E_10511\(1\).pdf](http://www.mit.gov.in/sites/upload_files/dit/files/GSR313E_10511(1).pdf).

²⁰⁰ Available at: <http://pib.nic.in/newsite/erelease.aspx?relid=74990>.

²⁰¹ Available at: <http://www.miit.gov.cn/n11293472/n11293832/n11293907/n11368223/13590447.html>.

the consent of the data subject should be obtained to the transfer of personal data to a third party. The export out of China of personal data is prohibited unless approved by government authorities or otherwise permitted by law. It is not clear how such a data export restriction would be applied or interpreted.

In July 2011, the Ministry of Industry and Information Technology of the People's Republic of China (the "MIIT") published draft rules (the "China ISP Rules") regulating the processing of personal information by Internet information service providers.²⁰² The draft China ISP Rules include many similar provisions to the China Personal Data Guidelines but, if passed into law, would be mandatory for Internet information service providers.

III. The Exposures Presented by Data Breaches

1. The Potential Costs and Damages of a Breach

The costs of a data breach include both the direct costs of immediate investigation, response, notification and remediation costs, and the indirect and at times longer-term costs of reputational damage and business interruption that can result from a publicized data breach. Costs of a breach can also often include liability to third parties whose personal information is acquired without authorization causing them financial detriment or who sustain other losses as a result of a data breach that can be attributed to the negligence of the breached entity. Even if such third-party claims do not ultimately succeed, they can involve very substantial litigation costs to defend. For publicly traded corporations, there is also often an effect on the stock price when a breach of their data security is reported and, as discussed above, recent SEC Guidance identifies cyber risks and incidents as potentially material information to be disclosed by publicly traded companies.

For insurers of companies that sustain a data breach, there are often claims under a variety of policies ranging from traditional general liability to D&O policies and some types of professional liability and errors and omissions policies, to specialty data breach and cyber risk policies, as insureds seek recovery of at least some of the substantial financial costs that they incur when they are involved in a data breach.

Costs per breach have recently been reported to have averaged in 2010 as much as \$214 per record,²⁰³ with the average total cost per company of more than \$7.2 million.²⁰⁴ A study focusing on 117 events covered by insurance and 77 events that had information as to claim payouts by insurers reported that the average cost for such data breaches was \$2.4 million.²⁰⁵

²⁰² Available at: <http://www.miit.gov.cn/n11293472/n11293862/n11301570/13978198.html>.

²⁰³ Ponemon Institute LLC, *2010 Annual Study: U.S. Cost of a Data Breach*.

²⁰⁴ *Id.*

²⁰⁵ NetDiligence, *supra*. The costs covered by this report versus other studies are not necessarily all the same, as this study focuses on payments made by insurers for covered costs, while many of the other studies include all costs, including the indirect costs of lost business.

Although averages may be driven up by a few enormous breaches, the unavoidable reality is that a breach results in substantial costs, due to mandatory reporting requirements for breaches involving Personal Information, the third-party claims that many breaches trigger, and the reputational damage to the entity sustaining the breach.

a. First-Party Costs

The range of immediate economic costs of entities sustaining a breach involving Personal Information often include:

Payment of forensic experts to find the cause of the breach and what needs to be done to stop it or prevent recurrence and evaluate if the cause was due to any non-compliance with applicable law or standards;

Obtaining legal advice on whether notice requirements are triggered and, if so, which ones and the types and content of notice required;

The cost of providing notice, including printing and mailing of letters;

The cost of providing a call center to answer inquiries by individuals receiving the notice;

The cost of credit monitoring services and identity theft insurance, if offered; and

Payment of public relations consultants for publicity control.

Additional significant costs to entities subject to PCI-DSS standards are the fines and penalties imposed under PCI-DSS if there is a failure to comply with their standards for protection of payment cardholder information, and related contractual fines and penalties.

Additionally, whether considered first or third party costs, breached entities are often subject to regulatory fines and penalties that may be imposed by regulatory agencies and states' attorneys general.

b. Third-Party Claims

Third-party claims by those who have allegedly been damaged by a data breach trigger longer-term costs, including substantial defense costs of the breached entity even when the claims are defeated.

(i) Consumer Claims

Consumer claims in the past have had limited success, as they face a number of obstacles. At the inception of a lawsuit, courts scrutinize whether the consumers have Constitutional standing to

pursue their claims. Courts will also analyze whether the consumers have sustained a legally cognizable injury. While many data breaches involve unauthorized access to Personal Information, affected individuals have not always been able to demonstrate that they sustained recoverable damages. Consumer plaintiffs may also have difficulty obtaining certification of their lawsuits as class actions, due to the highly individualized proof of loss required for each plaintiff.²⁰⁶ However, some recent decisions in 2011 have indicated that while consumers will likely still have difficulty ultimately prevailing in most claims absent demonstrated actual identity theft and resulting financial losses, defendants may not be able to obtain early pre-discovery dismissals of consumer claims as readily as they were in the past.

(1) Article III Standing

Often, consumer lawsuits based on breaches of Personal Information characterize the consumer's injury as the exposure of such data. Such lawsuits are typically pleaded as class actions and are therefore initiated in, or removed to, federal court pursuant to the Class Action Fairness Act.²⁰⁷ Once in federal court, the lawsuit must comply with the requirement of Article III of the Constitution that there be an actual "case or controversy" between the parties. Among the requirements for a "case or controversy" is that the plaintiff has suffered an injury in fact that is actual or imminent, not conjectural or hypothetical.²⁰⁸ In the absence of such an injury, the case is subject to dismissal based on a lack of standing.

Consumer claims based on the exposure of Personal Information have met mixed success at clearing the federal standing hurdle. A number of lower courts have dismissed consumer claims for a lack of standing, finding the alleged injury to be indefinite and speculative.²⁰⁹ In contrast, some federal appellate courts have found the standing requirement to be satisfied by allegations

²⁰⁶ As confirmed by a recent decision by the U.S. Supreme Court, *Wal-Mart Stores, Inc. v. Dukes*, 564 U.S. __ (June 20, 2011), there must be a certain degree of commonality amongst members of a plaintiff class, which requires more than an alleged violation of the same law (reversing class certification, noting that millions of employment decisions were in issue, and holding that "commonality requires the plaintiff to demonstrate that class members 'have suffered the same injury'" and that the common contention "must be of such a nature that it is capable of class wide resolution -- which means that determination of its truth or falsity will resolve an issue that is central to the validity of each one of the claims in one strike" and noting that the trial court is required to undertake a "rigorous analysis.")

²⁰⁷ 28 U.S.C. § 1332(d). The Class Action Fairness Act grants federal courts jurisdiction over class action lawsuits even in the absence of complete diversity between the parties, if certain other conditions are met.

²⁰⁸ See, e.g., *Friends of the Earth, Inc. v. Laidlaw Envtl. Servs., Inc.*, 528 U.S. 167, 180-81 (2000), citing *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992).

²⁰⁹ *Key v. DSW, Inc.*, 454 F.Supp.2d 684 (S.D. Ohio 2006); *Randolph v. ING Life Ins. & Annuity Co.*, 486 F.Supp.2d 1 (D.D.C. 2007); *Giordano v. Wachovia Sec. LLC*, 06-476, 2006 WL 2177036, 2006 U.S. Dist. LEXIS 52266 (D.N.J. July 31, 2006); *Bell v. Acxiom*, 06-485, 2006 WL 2850042 (E.D.Ark., Oct. 3, 2006); but see, *Claridge v. RockYou*, 09-cv-06032-PJH (N.D. Ca., April 11, 2011) (declining to dismiss, for lack of standing, plaintiffs' claim that they traded email and social media login credentials for access to applications, and that they lost the value of those credentials when the data was stolen by a hacker. The Court found case law regarding this "novel theory of damages" to be too scarce to dismiss on standing grounds, but left open a future standing challenge following discovery).

of an increased risk of future harm in the context of breaches of personal information.²¹⁰ Other federal appellate courts, however, have found that the “risk of future harm” presented by data breaches involving exposure of Personal Information is too speculative, and have held that persons whose information “may” have been accessed does not have standing, particularly in the absence of evidence suggesting that the data has been, or will ever be, misused.²¹¹

(2) Cognizable Injuries

Even if a consumer claim is deemed to satisfy the standing requirement, it may still be dismissible, or subject to an unfavorable ruling on summary judgment, if it fails to allege a cognizable injury under state law. In other words, the court may acknowledge that the plaintiff has pleaded a sufficient injury to satisfy Article III standing requirements, but conclude that applicable state law simply does not provide a remedy for such an injury.

One recent federal data breach case illustrates the obstacles that a consumer claim may face in this regard, and how the jurisdiction and the particular facts surrounding a claim can impact whether a consumer claim can survive dismissal on the pleadings. A federal district court, in a decision later reversed in part, initially dismissed a consumer class action due to lack of cognizable injury.²¹² The District Court had held that under the law of the state whose law governed (Maine), “if the merchant is not negligent, or if the negligence does not produce direct financial loss and instead causes only collateral consequences – for example, the customer’s fear that a fraudulent transaction might happen in the future, the customer’s expenditure of time and effort to protect the account, lost opportunities to earn reward points, or incidental expenses that the customer suffers in restoring the integrity of the previous account relationships – then the merchant is not liable.” The District Court had concluded that consumers who did not have a fraudulent charge actually posted to their account cannot recover.²¹³

²¹⁰ See *Krottner v. Starbucks Corp.*, 628 F.3d 1139 (9th Cir. 2010) (finding that plaintiffs had pleaded a “credible threat” of “real and immediate harm” stemming from the theft of a laptop containing their Personal Information); *Pisciotta v. Old Nat’l Bancorp.*, 499 F.3d 629 (7th Cir. 2007) (holding that plaintiffs’ allegation of increased risk of identity theft was sufficient to confer constitutional standing, despite the plaintiffs’ failure to plead financial loss or actual incidents of identity theft).

²¹¹ *Reilly v. Ceridian Corp.*, No. 11-1738 (3d Cir., December 12, 2011 (concluding that “allegations of hypothetical, future injury are insufficient to establish standing” and affirming dismissal of a complaint in which the putative class members alleged that as a result of a data breach involving personal information they had an increased risk of identity theft, incurred costs to monitor their credit activity, and suffered emotional distress). See also *Lambert v. Hartman*, 517 F.3d 433, 437 (6th Cir. 2008).

²¹² *In re Hannaford Bros. Co. Customer Data Security Breach Litigation*, 671 F. Supp. 2d 198 (D. Me. 2009, *rev’d*, *Anderson v. Hannaford Bros. Co.*, Nos., 10-2384, 10-2450 (1st Cir. Oct.20, 2011). But see *Rowe v. Unicare Life and Health Ins. Co.*, 09-CV-2286, 2010 U.S. Dist. LEXIS 1576 (N.D. Ill., January 5, 2010).

²¹³ The court allowed the case to proceed as to a single named plaintiff who had allegedly suffered a fraudulent charge that had allegedly not been removed from her account and which she had to pay. Subsequently, the parties filed a stipulation that the plaintiff in question had been fully reimbursed by her bank for the contested charges, which may effectively end the case depending on how the Supreme Judicial Court of Maine responds to the question recently certified from the federal court as to whether time and effort spent to avoid harm alone constitute cognizable injury. See also *Rowe v. Unicare Life and Health Insur. Co.*, 09-CV-2286, 2010 U.S. Dist. LEXIS 1576 (N.D. Ill., January 5, 2010), in which the court, citing the liberal pleading

On a motion of the plaintiffs for reconsideration and certification of legal questions to Maine's Supreme Judicial Court, the federal district court agreed to certify the following question to the state court:

Do time and effort alone, spent in a reasonable effort to avert reasonably foreseeable harm, constitute a cognizable injury under Maine common law?

The Maine Supreme Court answered the certified question in the negative, and held that under Maine law, in the absence of physical harm or economic loss or identity theft, time and effort alone spent in a reasonable effort to avoid harm do not constitute a cognizable injury for purposes of negligence or implied contract.²¹⁴ The federal court accordingly entered judgment in favor of the defendants on October 27, 2010.

The plaintiffs, however, appealed the decision to the United States Court of Appeals for the First Circuit, and in October 2011 the federal appellate court issued its decision, overturning the lower federal court decision as to certain categories of alleged damages, at least insofar as holding allegations were sufficient to withstand a motion to dismiss.

The First Circuit held that consumer claims for reimbursement of the cost of identity theft insurance and of fees for replacement of credit and debit cards following a breach of their personal information can be a cognizable injury under certain circumstances.²¹⁵ The court determined that certain categories of costs incurred by the plaintiffs were “reasonably foreseeable mitigation costs” and thus constitute a cognizable harm under Maine law. The court held, however, that not all mitigation costs in all circumstances would be recoverable, but rather, that plaintiffs need to show that the efforts to mitigate were reasonable, and that those efforts constitute a legal injury “such as actual money lost, rather than time or effort expended.”²¹⁶ The court noted that whether a mitigation cost is “reasonable” is a “contextual question.”²¹⁷

The First Circuit made a distinction between breaches involving inadvertently misplaced or lost data that has not been accessed or misused by third parties, from a large-scale criminal operation in which credit or debit card information was deliberately taken by sophisticated thieves intending to use the information to their financial advantage. Applying the facts before it, which included reported reports of actual fraud in that approximate 1,800 of the stolen card accounts had been used for fraudulent transactions, the court held that: “it was foreseeable, on these facts, that a customer, knowing that her credit or debit card data had been compromised and that thousands of fraudulent charges had resulted from the same security breach, would replace the

requirements of Illinois law, declined to dismiss common law and statutory claims related to the inadvertent disclosure of the plaintiffs' Personal Information on the Internet although there were no allegations of theft of Personal Information.

²¹⁴ *In re Hannaford Bros. Co. Customer Data Security Breach Litigation*, 2010 Me. 93, 4 A.D.3d 4920 (Maine 2010).

²¹⁵ *Anderson v. Hannaford Bros. Co.*, Nos. 10-2384, 10-2450, 659 F. 3d 151 (1st Cir. Oct. 20, 2011).

²¹⁶ *Ibid.*

²¹⁷ *Ibid.*

card to mitigate against misuse of the card data. ... Similarly, it was foreseeable that a customer who had experienced unauthorized charges to her account ... would reasonably purchase insurance to protect against the consequences of data misuse.”²¹⁸

The court also noted that “the principle of reasonableness” imposes a boundary on recovery of costs by claimants and noted, by way of example, that where neither the plaintiff nor those similarly situated have experienced fraudulent charges resulting from theft or loss of data, the purchase of credit monitoring services may be unreasonable and not recoverable. It also affirmed the lower court’s holding that there can be situations in which there is no foreseeable loss as a matter of law. Therefore, the court upheld the district court’s finding that damages such as loss of award points and change fees for pre-authorized credit transactions are not foreseeable and not compensable.

Other courts have held that a claim for credit monitoring costs following a theft of a laptop or other computer hardware containing Personal Information, without evidence that the information had been accessed or used, is alone not sufficient to sustain a claim for negligence under applicable common law.²¹⁹

²¹⁸ 659 F. 3d at 165. For an analysis of the First Circuit’s recent decision in *Hannaford Bros. Co.*, see “Foreseeable and Reasonable Mitigation Costs Can Constitute Cognizable Injury from a Data Breach - At Least Under Maine Law,” *Edwards Wildman Palmer Client Advisory*, October 2011, <http://www.edwardswildman.com/newsstand/detail.aspx?news=2659>.

²¹⁹ See, e.g., *Hammond v. The Bank of New York Mellon Corp.*, Case No. 1:08-CV-06060 (S.D.N.Y. June 25, 2010) (granting defendant’s motion for summary judgment on claims of negligence, breach of fiduciary duty, breach of implied contract, and state consumer protection law claims concerning the theft from the defendant of computer backup tapes containing Personal Information of the plaintiffs; the court held that the plaintiffs lack Article III standing because their claims of increased risk of future harm are “future-oriented, hypothetical, and conjectural,” and thus there is no case or controversy); *Ruiz v. Gap, Inc. and Vangent Inc.*, 2009 WL 941162 (N.D. Cal., April 6, 2009) (granting defendants’ motion for summary judgment of claims for negligence and breach of contract seeking compensation for credit monitoring services, which claims arose from theft of laptop computers from the offices of a vendor of Gap that processed job applications, resulting in loss of Personal Information of plaintiffs; the court held that under California law, the increased risk of future theft did not arise to the level of appreciable harm necessary to assert a negligence claim, and his assertion that his credit monitoring costs were a compensable attempt to mitigate damages failed because he had not damages to mitigate since he had never been a victim of identity theft); *Caudle v. Towers, Perrin, Forster & Crosby, Inc.*, 580 F. Supp. 2d 273 (S.D. N.Y. 2008) (the court dismissed the claim for negligence and breach of fiduciary duty brought by an employee against his employer’s vendor who lost the laptop; however, the court did allow to go forward the claim for breach of contract to allow discovery on the issue of whether the employee was a third-party beneficiary of the contract between his employer and the vendor under the terms of the contract; the plaintiff had withdrawn his other claims for misrepresentation and breach of privacy); *Shafraan v. Harley Davidson, Inc.*, 2008 WL 763177 (S.D.N.Y. 2008) (granting motion to dismiss claims for future credit monitoring arising from loss of a laptop containing Personal Information, and noting that “courts have uniformly ruled that the time and expense of credit monitoring to combat an increased risk of future identity theft is not, in itself, an injury that the law is prepared to remedy”). These decisions also identify case law in other jurisdictions addressing the issue of what is a legally cognizable injury of an individual whose Personal Information as breached, but who has not sustained actual identity theft or financial loss; *Stollenwerk v. Tri-West Health Care Alliance*, 254 Fed.Appx. 664 (9th Cir. 2007) (upholding summary judgment against plaintiffs whose PI was contained on a stolen hard drive, and denying credit monitoring costs as damages, as the plaintiffs did not claim any actual misuse of their PI). See also, *Randolph v. ING Life Ins. and Annuity Co.*, 486 F.Supp.2d. 1 (D.D.C., 2007) (finding that the plaintiffs’ increased risk of identity theft and the cost of protecting against identify theft, following the theft of a laptop containing their private Personal Information, did not rise to the level of an “injury in fact” for constitutional standing purposes).

Statutory claims, however, may provide an avenue for recovery related to the time and expense involved in protecting personal data and credit accounts (or for other theories of injury). For example, one federal decision construing the Federal Trade Commission Act (“FTCA”) found that such lost time and expense constitutes “substantial injury” under the FTCA.²²⁰ Courts construing state unfair trade practice or consumer protection statutes, which often expressly rely on interpretations of the FTCA,²²¹ may apply such reasoning to data breach cases brought pursuant to those state statutes. A recent federal decision found that class action plaintiffs had pleaded a “sufficient injury” under California’s Consumers Legal Remedies Act when they alleged that the defendant disclosed highly sensitive Personal Information; the statute requires only that a consumer has suffered “any damage,” defined by California decisions as a “low but nonetheless palpable threshold of damage.”²²² Another recent federal decision interpreting California law, however, limited plaintiffs’ potential recovery by requiring that all members of a class action establish a pecuniary loss resulting from a data breach or privacy violation.²²³

Plaintiffs in data breach cases continue to develop their strategies and theories of liability. Newer theories include claims for negligent misrepresentation based on inaccuracies in notice letters as to the breach or any continuing risk, or in communications from call centers established by the breached entity. Taking a different approach, one academic recently commented on the “surprisingly good” fit between product liability law and privacy, particularly in the area of social media.²²⁴ Under this approach, a plaintiff may assert that unreasonable risks to the security of Personal Information created by a defendant’s product (which may be a website) resulted from a design defect. While many of these theories have yet to be tried and tested, as this area of law develops and breaches continue, plaintiffs’ lawyers will undoubtedly explore new theories of recovery.

(3) Class Certification

Yet another obstacle to consumer claims is the prospect that the consumer’s application for class certification may be denied. The losses claimed by an individual consumer will generally be

²²⁰ *FTC v. Neovi, Inc.*, 598 F.Supp.2d 1104, 115 (S.D. Cal. 2008) (finding that the affected consumers “often spent a considerable amount of time and resources contesting the checks at their banks, protecting their accounts, and attempting to get their money back” and that “the time consumers spent in these efforts was valuable”), *aff’d*, 604 F. 3d 1150 (9th Cir. 2010).

²²¹ *See, e.g.*, C.G.S. § 42-110b; 5 M.R.S.A. § 207(1).

²²² *Doe I v. AOL LLC*, 719 F.Supp.2d 1102 (N.D. Ca. 2010).

²²³ *In re Google Inc. Street View Electronic Communications Litigation*, 5:10-md-02184-JW (N.D. Ca.) (June 29, 2011). Plaintiffs in that case argued that Google used sophisticated equipment not available to the public when taking photographs to be incorporated in its Google Maps and Google Earth programs in order to determine what websites were being visited by users whose data had been collected. They claimed that Google violated wiretapping statutes and laws and that Google’s actions constituted an unfair and deceptive trade practice in violation of California law. The court denied Google’s motion to dismiss the federal wiretapping claim, granted the motion to dismiss the state wiretap claims and granted the motion to dismiss the unfair and deceptive trade practice claim. Under this decision, each individual class member will need to demonstrate their own pecuniary damages in a privacy-related class action, which could make class certification difficult in privacy cases.

²²⁴ James Grimmelman, *Privacy as Product Safety*, 19 *Widener L.J.* 793 (2010).

minimal. On the other hand, certification of a class of thousands, or millions, of affected consumers can multiply such losses and thereby create the incentive for plaintiffs' lawyers to pursue litigation.

One federal case²²⁵ demonstrates that certification can be a difficult hurdle that is not easily overcome. The lawsuit was based on allegations that a contractor managing a government-run healthcare plan had computer drives containing personal information stolen from its offices. One of the plaintiffs, who had suffered an actual monetary loss resulting from an identity theft, filed a motion for class certification. The court denied the motion. First the court noted that several other plaintiffs, who had not suffered actual loss, had been dismissed from the case. Then, examining the standard for certifying a class action, the court found that the remaining plaintiff failed the test of adequacy, a requirement for class certification, in that he was not an adequate representative of the class. The remaining plaintiff's injuries were not similar to those suffered by other class members, who had not suffered monetary loss from actual identity theft. The court also found that the remaining plaintiff failed the test of predominance, another requirement of class certification, because he failed to show that questions of fact and law common to class members predominate over questions affecting only individual members. The court reasoned that individual issues related to proof of causation, i.e., determining whether the breach actually caused the identity theft, would predominate over any common issues.²²⁶

(ii) Bank Claims

Added to the list of potential third-party claims are efforts by banks and credit unions that sustained losses as a result of their customers' payment cards being cancelled and replaced, and of fraudulent charges they absorbed, to recover such financial losses from the entity breached. While often consumers cannot demonstrate actual financial loss if they did not sustain or pay unauthorized charges, banks have been increasing pressure on state and federal lawmakers as well as courts to allow them the right to reimbursement from breached entities for the costs banks sustain from absorbing fraudulent charges and reissuing debit and credit cards.

While initially the legal basis for efforts by banks and other financial institutions to recover their costs from a breached company were very limited, efforts are underway to provide routes for legal recourse. As noted above, Washington State passed legislation that provides for liability of a credit or debit card processor or business to a financial institution if the processor or business fails to take reasonable steps to guard against unauthorized access to account information that is in its possession, and such failure is found to be the proximate cause of a breach. Similarly and as also discussed above, the Minnesota Plastic Card Security Act provides that financial

²²⁵ *Stollenwerk v. TriWest Healthcare Alliance*, No. 03-0185 (D.Ariz., June 10, 2008).

²²⁶ *See also, Wal-Mart Stores v. Dukes, supra* (in which the U.S. Supreme Court, in a 2011 decision, reversed class action certification, on the grounds that there was no sufficient commonality in an employment discrimination matter that involved millions of employment decisions, and noting that the trial court is required to undertake a "rigorous analysis.")

institutions may recover from a company that accepts payment cards if the company retains card security code data, PIN verification code numbers or the full contents of any track of magnetic stripe data for longer than 48 hours after authorization of a transaction and there has been a security breach exposing payment card data.

A pair of cases illustrates the courts' approach to whether such claims by banks constitute cognizable injuries under common law, and what causes of action courts are likely to recognize.

In the first of these,²²⁷ the First Circuit Court of Appeals held that, under Massachusetts law, banks issuing credit and debit cards to customers who subsequently had that card information stolen from a merchant's computer systems and used for fraudulent transactions, stated a claim against the store operator and the bank serving as its "processing bank" for the store's payment transactions. The banks had claimed that both the merchant and its processing banks were negligent in failing to follow PCI-DSS security protocol and in delaying in providing notice after the breaches had been discovered, and that as a result they had sustained financial losses from reimbursing the customers for fraudulent charges, monitoring their accounts, and cancelling and reissuing payment cards. Their complaint included claims for negligence, breach of contract, and unfair or deceptive practices, and also sought to assert a claim for conversion. The First Circuit upheld the denial of the dismissal of the negligent misrepresentation claim that was based on the argument that by accepting and processing credit card transactions, the merchant and its processing bank impliedly represented that they would comply with MasterCard and Visa data security requirements, although it noted that "the present claim survives, but on life support." Similarly, the claim for unfair or deceptive trade practices survived dismissal, but primarily based on the lack of discovery of the defendant's conduct in issue and with reference to the merchant's argument for dismissal having to "await discovery and perhaps a summary judgment motion." However, the dismissal of the tort-based negligence claim was upheld on the grounds that Massachusetts, like so many states, holds that "purely economic losses are unrecoverable in tort and strict liability actions in the absence of personal injury or property damage." Efforts by one bank to claim "property damage" based on property interest in the payment card information failed on the grounds that it was not a result of physical destruction of property. The dismissal of the breach of contract claim was also upheld, as while the merchant and its processing bank had agreements with Visa and MasterCard to comply with certain security procedures, the claimant banks were not parties to those contracts and did not demonstrate that they were third-party beneficiaries of those contracts. The First Circuit also upheld the denial of the addition of a claim for conversion, although in wording that arguably left the door open for it to be more successfully pleaded in another matter. Subsequent to the First Circuit's decision, the remaining parties settled their claims and the District of Massachusetts dismissed the case on September 11, 2009.

²²⁷ *In Re TJX Companies Retail Security Breach Litigation*, 564 F.3d 489 (1st Cir. 2009) (as amended on rehearing in part May 5, 2009).

In the second case,²²⁸ the Supreme Judicial Court of Massachusetts reached a similar decision when it upheld two lower court decisions dismissing claims by credit unions and their insurer for damages arising from an alleged data security breach in which third parties obtained and fraudulently used debit and credit card information of cards issued by the credit unions, for which fraudulent charges the credit unions reimbursed their customers and the credit unions' insurer then reimbursed the credit unions. Like the First Circuit, the Supreme Judicial Court of Massachusetts upheld dismissal of the third-party beneficiary contract claims because the plaintiffs could not show that they were intended beneficiaries, and upheld dismissal of the negligence claims under the economic loss doctrine. With regard to claims for fraud and negligent misrepresentation, which were based on allegations that in accepting credit and debit cards for payment the defendants represented that they were in compliance with Visa and MasterCard regulations prohibiting them from storing data, the court upheld summary judgment dismissing those claims after finding that the plaintiffs had never seen the defendants' agreements with Visa and MasterCard and thus they could not establish that the defendants' representations induced them to become or remain card issuers. The court also found that the plaintiffs could not establish that they would have altered their participation in the card system after becoming aware of the defendants' breach. Additionally, the court found that any reliance on the alleged representations would have been unreasonable.

Banks continue to pursue litigation against companies that have suffered data breach of debit and credit card information. After Heartland Payment Systems, a processor of debit and credit card transactions, reported that debit and credit card data had been stolen from its system, a number of banks filed lawsuits against Heartland. The federal lawsuits have been consolidated and centralized in the Southern District of Texas,²²⁹ and the plaintiffs are asserting claims for negligence, negligence *per se*, negligent and intentional misrepresentation, violation of consumer protection statutes, and breach of contract. Heartland filed a motion to dismiss all of the claims against it, citing the decisions in *Cumis* and *TJX* in support. Recently, the U.S. District Court for the Southern District of Texas decided the motion to dismiss the claims of the Financial Institution plaintiffs, which were nine issuer banks (banks that provided the credit/payment cards to consumers) that alleged that the data breach resulted from a failure by Heartland to follow industry security standards (PCI-DSS), resulting in the issuing banks incurring significant expenses replacing payment cards and reimbursing fraudulent transactions. The court granted the Heartland motion to dismiss in part, and denied it in party, holding that (1) the claims for negligence and violation of New Jersey, New York and Washington states' consumer protection laws were dismissed with prejudice; (2) the claims for breach of contract, breach of implied contract, express misrepresentation, negligent misrepresentation based on nondisclosure, and violation of California, Colorado, Illinois and Texas consumer protection statutes were dismissed

²²⁸ *Cumis Insurance Society, Inc. et al. v. BJ's Wholesale Club, et al.*, 918 N.E.2d 36 (Mass. 2009).

²²⁹ *In re Heartland Payment Systems Inc. Customer Data Security Breach Litigation*, 09-MD-2046-LHR (S.D. Tex.).

without prejudice and with leave to amend; and (3) the motion to dismiss the claims brought under the Florida Deceptive and Unfair Trade Practices Act was denied.²³⁰

While banks have struggled to avoid dismissal of common law claims, the legislation passed in states such as Washington, Nevada and Minnesota, discussed above, is providing banks with statutory grounds for seeking damages even where common law grounds may fail.

(iii) Other Third-Party Claims

As breaches continue, an increasing range of potential third-party claims can be expected, by regulators and by individuals and entities purportedly affected by breaches.

Attempts by those allegedly sustaining collateral damage from a data breach resulting in credit card cancellations is demonstrated by one case in which, as a result of a large data breach sustained by a grocery chain, a group of unrelated merchants sought to recover from the grocer on the basis that these other merchants suffered business losses due to the resulting mass cancellation of credit and debit cards.²³¹ While that attempt was unsuccessful, ever new types of claims are likely to be forthcoming.

2. Industries Exposed

While large-scale data breach incidents in recent years have been front-page news, there are hundreds of other data breach incidents each year in the United States alone, affecting companies in a broad range of industries.²³² Indeed, any entity that has Personal Information in its possession, whether that of employees, customers, clients, or other third parties, is a potential target for data breaches, either malicious or accidental. Companies with intellectual property or other confidential business information can also be a target of espionage, and indeed trade secrets and confidential business information is reported to be increasing as a target.²³³ Moreover, every company is also susceptible to the more garden-variety of data breaches resulting from lost laptops, PDAs and smartphones, improperly disposed of paper records, transfer of unencrypted information that simply gets lost, and lack of protective measures of vendors retained by a company to provide services that include the vendor being provided with Personal Information.

Recent studies of data breaches note that cyber criminals are increasingly targeting points of data concentration to acquire large amounts of consumer information, such as personal identification

²³⁰ *In re Heartland Payment Systems, Inc. Customer Data Security Breach Litigation/Financial Institution Track Litigation*, MDL No. 09-2046 (December 1, 2011).

²³¹ *In re Hannaford Bros Co. Customer Data Security Breach Litigation*, Docket No. 2:08-md-01954-DBH (D. Me.).

²³² This does not include the vast number of incidents where personal information is stolen directly from individuals, or in which the data breach involves theft of information that does not qualify as Personal Information subject to mandatory reporting.

²³³ *Underground Economies*, *supra*.

numbers (PIN) with associated debit and credit card numbers, usually for resale.²³⁴ Social Security numbers are a main target, due to their usefulness in identity theft and the fact that, unlike credit card numbers, they are not easily cancelled and removed from usage.

The following is a representative sampling of recent publicly reported breaches, demonstrating the range of industries susceptible. These focus on the larger breaches.²³⁵

a. Retailers

Retailers, because of their heavy use of credit and debit card transactions, have long been a target of cyber criminals seeking credit and debit card numbers. According to one report of a “counter threat unit,” data breaches against retailers were up by 43% from January to September 2011.²³⁶ That counter threat unit asserted it had stopped 91,500 attackers per retail customer in the first nine months of 2011, compared to 63,581 from April through December 2010.²³⁷

On-line retailers are a target, as well as more traditional bricks and mortar companies. This is demonstrated by the massive breach reported in April 2011 of Sony Playstation’s video game online network, with credit card and other information of over 100 million customers reportedly accessed, although the scope of access to Personal Information has yet to be finally determined. Within only a few weeks of reporting the breach, Sony was faced with dozens of lawsuits and a Congressional investigation.²³⁸

Other examples are:

Michaels Stores (May 2011) – Approximately 90 PIN pads located at stores in 20 states were found to have been tampered with, reportedly compromising debit and credit card information of an unknown number of customers.

Macy’s St. Louis (February 2010) – According to news reports, in February 2010, documents containing Social Security numbers and credit/debit card numbers were found in a dumpster outside Macy’s St. Louis store, being used by a homeless person for a bed and blowing in the wind.

²³⁴ Verizon DBIR, 2010, *supra*. The United States Secret Service noted in the DBIR that the cost of purchasing stolen credit card data ranges from \$1 to over \$10 per credit card, depending upon the amount of additional Personal Information that is included.

²³⁵ Most of the incidents listed were derived from the Chronology of Data Breaches maintained by the Privacy Rights Clearinghouse, a nonprofit consumer advocacy organization, at www.privacyrights.org/ar/ChronDataBreaches.htm and from the Identity Theft Resource Center at www.idtheftcenter.org. See also www.datalossdb.org.

²³⁶ Dell SecureWorks®, *Hacker Attacks Targeting Retailers Up 43%*, at http://www.secureworks.com/research/counter_threat_unit/.

²³⁷ *Id.*

²³⁸ Lori Chordas, *Sony to Offer \$1M Insurance Policies to US Gamers Impacted by Massive Cyber Breach*, BestWire Services, May 11, 2011.

TJX (January 2007) – An intrusion into the computer system that processes and stores customer transactions resulted in the theft of 45.7 million credit and debit card numbers.

The TJX breach, one of the early large reported data breaches, demonstrates the wide range of costs and exposures that a large data breach of a retailer can present. TJX was faced with consumer class actions as well as bank and other third-party claims. Their costs included settling consumer lawsuits for \$6.5 million in attorneys' fees, plus compensation to consumers for time they lost as a result of the intrusion up to \$60 and, in some cases, vouchers, credit monitoring and identity theft insurance. Additional lawsuits were filed by banks and other financial institutions who allegedly sustained losses as a result of the unauthorized access to consumer credit card numbers and their subsequent cancellation and replacement. TJX also entered into a \$9.75 million settlement with the attorneys general of 41 states, with portions of the amount to go into consumer protection funds and to reimburse costs of the investigation. The computer hacker who helped organize the breach was sentenced to 20 years in prison.²³⁹

b. Hospitality/Food and Beverage

The heavy use of credit and debit card transactions in these industries, which include hotels, restaurants, and food retailers, makes them a target for cyber criminals as well as more garden variety theft or inadvertent disclosure of Personal Information. According to one study, 38% of the breaches involving credit cards in 2009 had targeted hotels, and 13% targeted restaurants.²⁴⁰ For restaurants and others in this industry, breaches can simply be the result of careless use or disposal of credit and debit card information, or it can be that they are the target of cyber criminals seeking to obtain credit and debit card numbers as they are transmitted by customers for payment. Further, this industry like all others is susceptible to lost laptops and other breaches of security involving employee and client Personal Information. Some recent examples of larger breaches include:

Margarita's Restaurant (July 2011) – A payment-card data breach at this Huntsville, Texas restaurant was likely caused when the restaurant's point-of-sale system was infected with a virus after a third-party vendor's network was hacked.

San Diego Hotel (September 2010) – Malware uploaded to a hotel chain captured the credit card information of an unknown number of people; the card numbers were reportedly used to make fraudulent charges in central Florida.

²³⁹ Reported in the *Boston Globe*, March 26, 2010.

²⁴⁰ Joe Sharkey, *Credit Card Hackers Visit Hotels All Too Often*, The New York Times, July 5, 2010 (citing study released by SpiderLabs); see also, *Hospitality Industry Data Theft: Hotel Owners Must Prevent Breaches of Credit Card Processing Systems* at hospitalityrisksolutions.com, August 7, 2010.

Multiple Restaurants (September 2010) – Thieves paid servers at a number of Washington, D.C. area restaurants to run an unknown number of customers' credit cards through skimming devices.

Emily Morgan Hotel (July 2010) – Thieves obtained stacks of credit card receipts from a hotel storage room, stealing 17,000 records and making hundreds of thousands of dollars in fraudulent charges.

Briar Group, LLC (October 2009 breach; 2011 Attorney General fine) – Over 125,000 credit and debit card numbers were reportedly compromised after computer systems used to process cards for Briar Group, which operates restaurant chains, were infected with malware. In March 2011, the Massachusetts Attorney General reached an agreement under which Briar Group would pay \$110,000 in penalties in connection with the breach.

Mad Capper Saloon & Eatery (April 2009) – About 80 complaints of compromised credit cards were connected by police to the use of the cards at a restaurant. The restaurant owner reported being unable to identify the source of the problem, despite an extensive investigation.

Nashville Hotels (2009) – In 2009, after more than eight months of investigation, investigators discovered that thieves were accessing credit card information by dumpster diving.

Rio Grande Food Project (February 2009) – A laptop containing Personal Information, including Social Security numbers, of tens of thousands of clients of a food pantry was stolen.

Starbucks (October 2008) – A laptop containing Personal Information on 97,000 employees was stolen.

Hannaford Bros. (March 2008) – The placing of “malware” into this supermarket chain's payment-processing software led to the theft of 4.2 million records, including credit and debit care numbers, expiration dates and PINs.

Kraft Foods (March 2008) – A laptop containing names and possibly Social Security numbers of 20,000 employees was stolen from an employee of Kraft Foods who was traveling on company business.

c. Universities and Other Educational Institutions

Universities have been one of the major sources and targets of data breaches, as have lower-level educational institutions. This may be because of the large number of computer terminals accessible by a myriad of students and employees, the mischievousness of students, a more casual attitude towards computer security at some educational institutions, or the fact that many universities have research facilities and programs whose information is a target for those wanting

unauthorized access. According to one report, in 2010 there were 65 reported data breaches, affecting over 1.6 million records, at educational institutions alone.²⁴¹

Some examples of reported breaches involving educational institutions are:

Yale University (August 2011) – The names and Social Security numbers of 43,000 people affiliated with the university reportedly had been publicly viewable on Google for the prior 10 months. The breach purportedly occurred when Google modified its search engine to make it capable of finding and indexing file transfer protocol (FTP) servers.

University of South Carolina (March 2011) – A computer security breach exposed the Social Security numbers and other private information of nearly 31,000 faculty, staff, retirees and students.

St. Louis University (March 2011) – Hackers accessed the University's network, obtaining Personal Information, including Social Security numbers, of almost 13,000 students and current and former employees and contractors.

Ohio State University (December 2010) – Unauthorized individuals gained access to a server containing the personal information, including an unknown number of Social Security numbers, of up to 760,000 people associated with the university.

University of Hawaii West Oahu (October 2010) – Unencrypted files placed on the faculty web server by a faculty member exposed Personal Information, including Social Security numbers, of over 40,000 alumni. In November 2010, an alumnus of the university filed a class-action lawsuit against the university, alleging that he was affected by the breach and an earlier one in June 2009, and that his Social Security number had been compromised.

University of North Florida (September 2010) – A hacker, possibly from overseas, gained access to Personal Information, including Social Security numbers, of up to 107,000 students, potential students and employees.

Valdosta State University (March 2010) – An unidentified hacker infiltrated a server and gained access to the Personal Information, including Social Security numbers of up to 170,000 students and faculty.

Columbia University (January 2010) – According to news reports, Columbia University had three laptops containing Personal Information of 1,400 Columbia University affiliates stolen from University offices, with Social Security numbers included.

²⁴¹ Identity Theft Resource Center, *2010 Data Breach Stats*.

University of Central Missouri (2009) – In early 2009, the University notified 7,000 students after two computer reports were stolen that contained the names, Social Security numbers and dates of birth of students enrolled for the summer of 2005 and the summer of 2006.

Cornell University (2009) – In 2009, Cornell reported that a computer was stolen containing the names and Social Security numbers of over 45,000 current and former students, faculty and staff members.

Texas A&M Corpus Christi (2008) – The university reportedly discovered in late 2008 for the fourth time in two years, and the second time in two months, that there was a security breach that exposed current and former students' Social Security numbers. A student apparently conducted an Internet search on the university's website and viewed a document that listed admissions applicants from 2005, listing 1,430 names and Social Security numbers.

d. Healthcare Providers and Health Insurers

The healthcare industry reportedly has one of the highest rates of breaches. The U.S. Department of Health and Human Services reports that as of mid-November 2011, the number of breaches of patient Personal Information affecting 500 or more people since it began keeping records in 2009 reached 364, with more than 17 million individuals' records affected.²⁴² Three of the top six most significant data breaches of 2011 reportedly took place in the healthcare industry.²⁴³ Data breaches have reportedly cost the U.S. healthcare industry \$6.5 billion annually.²⁴⁴ One recent study reports that breaches involving healthcare institutions are still growing in number, with the estimated cost per benchmarked organization estimated at \$2,243,700.²⁴⁵

The loss rate of customers following a healthcare breach is reportedly more than twice as much as, for example, a retail breach, as consumers have a higher expectation of protection and privacy of their healthcare records.²⁴⁶ Healthcare insurance identification is apparently worth many times more than payment card information on the black market and this makes healthcare institutions a target. According to one research firm, criminals tend to use information stolen from medical records for an average of 320 days versus 81 days for data stolen from other

²⁴² *HIPAA & Breach Enforcement Statistics for December 2011*, produced by Health Information Privacy/Security Alert, published by Melamedia, LLC. See also Brian T. Horowitz, *Health Care Data Breaches Affect 10 Million Patients Since Fall 2009*, eWeek.com, April 29, 2011 <http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html>.

²⁴³ *Privacy Right Clearinghouse*, Healthcare Finance News, December 19, 2011 (identifying the three significant breaches those of Sutter Physicians Services/Sutter Foundation, Healthnet, and Tricare Management).

²⁴⁴ Healthcare Finance News, December 1, 2011

²⁴⁵ Ponemon Institute *Second Annual Benchmark Study on Patient Privacy and Data Security*, December 2011.

²⁴⁶ Ponemon Institute, *2009 Annual Study*, *supra*.

sources, and it takes twice as long to detect a medical data breach compared with other kinds of thefts of Personal Information.²⁴⁷

Data breaches involving healthcare institutions and health insurers can range from simple loss of a laptop,²⁴⁸ to systemic electronic data breach of patient Private Information, to a reported incident of a worm infecting medical equipment run with the assistance of computer systems. A concern with compromise of medical center systems that is not an issue with most other industries is that it has the potential to negatively affect patient care, either directly affecting operation of equipment or by interrupting the systems that provide information used in the rendering of care, with resultant bodily injury.

Reported incidents include:

UCLA Health System (November 2011) – UCLA Health System notified thousands of patients that their personal information was stolen and they are at risk of possible identity theft. Altogether, 16,288 patients' information was reportedly taken from the home of a physician whose house was burglarized.

Tricare (October 2011) – Tricare, the managed care arm of the U.S. government's Military Health System, disclosed that a contractor, Science Applications International Corp. (SAIC), had lost or had stolen from it backup tapes containing personally identifiable information, including some health data, of about 4.9 million people. The tapes contained data from electronic health records (EHRs) used at military hospitals, clinics, and pharmacies in the San Antonio area from 1992 until September 7, 2011.

Sutter Physicians Services/Sutter Medial Foundation (October 2011) – A company-issued desktop computer was stolen, reportedly exposing more than 4 million patients' records.

North Memorial Health Care (September 2011) – The theft of a laptop computer filled with thousands of patient records triggered a federal investigation of Fairview and North Memorial hospitals in Minnesota.

Health Net Inc. (March 2011) – A number of data servers containing the patient Personal Information, including Social Security numbers, of 1.9 million people went missing from a California data center.

New York City Health and Hospitals Corporation (February 2011) – Computer backup tapes containing health information of up to 1.7 million patients were reported stolen.

²⁴⁷ Neil Versel, *Report: Medical data theft growing as more adopt EMRs*, www.fierceemr.com (April 1, 2010).

²⁴⁸ Laptop theft is reportedly the most prevalent cause of breaches of PHI affecting more than 500 people. Mary Mosquera, *Laptop thefts top cause of health data breaches*, Government Health IT, November 12, 2010.

Keystone Mercy Health Plan and AmeriHealth Mercy Health Plan (October 2010) - A portable computer drive containing the names, addresses, and health information of 280,000 Medicaid members in Pennsylvania was lost at the corporate offices of the two affiliated insurers.

Martin Luther King, Jr. Multi-Service Ambulatory Care Center (September 2010) – A janitor sold 14 boxes containing the medical records of 33,000 patients to a recycling center.

University of Pittsburgh Medical Center (September 2010) – The Justice Department announced that a former employee of UPMC Shadyside Hospital had been indicted on charges of using PHI for personal gain in violation of HIPAA. According to the indictment, which was filed in the United States District Court for the Western District of Pennsylvania, the employee used the information to file false tax returns.

South Shore Hospital, South Weymouth, Massachusetts (July 2010) – Computer backup files containing Personal Information of as many as 800,000 patients, employees, donors, volunteers, and vendors may have been lost in transit to a data management vendor which was to have destroyed the files.

WellPoint (June 2010; settlement July 2011) – About 470,000 customers in ten states were notified of a breach that exposed Personal Information, including, potentially, Social Security numbers and credit card numbers. Part of the breach involved the online application program through which applicants can track the status of their applications. In September 2010, a WellPoint applicant whose information was exposed by the breach filed a class action lawsuit against WellPoint in California. In October 2010, the Office of the Attorney General of Indiana announced that it was suing WellPoint due to a delay in notification of the breach. In July 2011, a settlement was reportedly reached under which WellPoint paid the State \$100,000 and the suit was dismissed.

Affinity Health Plan (April 2010) – A managed care service notified more than 400,000 current and former customers and employees that their Personal Information may have been contained on a hard drive in a digital copier. The managed care service leased the copier and returned it to the leasing company without erasing the hard drive.

Griffin Hospital (February 2010) – A radiologist fired from the Derby, Connecticut hospital used his former co-workers' passwords to access the files of hundreds of patients in order to offer them services at a different hospital. The records contain the patients' names, exam dates, exam descriptions, gender, age, medical record numbers and dates of birth.

BlueCross BlueShield of Tennessee (January 2010) – Personal Information of nearly one million plan members, including hundreds of thousands of Social Security numbers, was

compromised when 57 hard drives were stolen. The insurer faces an estimated \$10 million in costs associated with the data breach.

Health Net (November 2009) – The Connecticut Attorney General began an investigation of Health Net in November 2009 in connection with a lost portable external hard drive that contained the Personal Information of 1.5 million customers, 446,000 of which were Connecticut residents. The investigation centered on why the company took six months after allegedly learning of the incident to provide notification to affected individuals. On January 13, 2010, the Connecticut Attorney General filed a lawsuit against Health Net alleging that Health Net failed “to secure private patient medical records and financial information involving 446,000 Connecticut enrollees and [for failing to] promptly notify consumers endangered by the security breach.”²⁴⁹ On July 6, 2010, Health Net consented to a Stipulated Order with the Connecticut Attorney General and the State of Connecticut under which Health Net agreed to (i) pay \$250,000 to Connecticut, (ii) offer two years of credit monitoring for affected individuals, (iii) obtain \$1 million of identity theft insurance, and (iv) reimburse affected individuals for security freezes. Health Net also agreed to a corrective action plan that bring it into compliance with HIPAA requirements. In November 2010, the Connecticut Insurance Department announced that Health Net had agreed to pay a \$375,000 fine in connection with the breach.

Anthem Blue Cross and Blue Shield of Connecticut (November 2009) – A laptop was stolen that contained Personal Information of nearly 850,000 healthcare professionals, 19,000 of which were Connecticut residents.

Medical Equipment (reported in the press June 2009) – A computer worm reportedly infected medical equipment in hospitals around the world.

Virginia Hospital (April 2009, according to press report) – Hackers accessed 8.5 million patient prescription records in a Virginia hospital, deleting backups and issuing a ransom note.

e. Financial Institutions

Financial institutions remain a major target of cyber criminals due to the volume and nature of the information they collect and maintain, as well as less malicious disclosures. Some publicly reported examples are:

Citigroup (June 2011) – Its servers were hacked into and the names, addresses account numbers and other account information of 200,000 credit card customers were stolen.

²⁴⁹ The Connecticut Attorney General’s press release on the lawsuit is available at <http://www.ct.gov/ag/cwp/view.asp?A=2341&Q=453918&pp=12&n=1>.

GunnAllen Financial (April 2011) – Two former employees of an investment brokerage were fined \$20,000 each by the Securities and Exchange Commission for transferring account information regarding 16,000 clients to a new employer. The fines were levied for violation of the Safeguard Rule, under which SEC-regulated institutions are required to give customers the opportunity to “opt out” of having their information shared with unaffiliated third parties.

Educational Credit Management Corporation (March 2010) – A thief stole two safes containing Personal Information of 3.3 million student loan recipients. The data, contained on 650 DVDs, was housed in a building that was supposed to be secure.

New York Mellon Corp. (October 2009) – A computer technician was charged with stealing the identities of more than 150 bank employees and using the stolen identities to steal more than \$1.1 million from charities, non-profits and other groups.

Bank of America (September 2008) – A group of four people was reportedly suspected of illegally obtaining ATM card numbers by using card skimmer devices attached to about 10 Bank of America branches.

Wachovia Bank (August 2008) – A skimming device placed on an ATM collected debit card information, allowing a criminal to create new debit cards containing the stolen information.

Countrywide Financial Corp. (August 2008) – A senior analyst at Countrywide’s subprime lending division was arrested by the FBI and accused of selling Personal Information, including Social Security numbers, of two million Countrywide customers over a two-year period.

Bank of New York Mellon (March 2008) – A box of data storage tapes containing Personal Information, including Social Security numbers and possibly account numbers of up to 12.5 million customers, was lost.

Ameritrade (September 2007) – Ameritrade announced that the names, addresses, phone numbers and trading information of millions of customers at that time had been compromised by an intrusion. The stolen information was later used to spam them. Social Security numbers were reportedly not compromised, but the breach received media attention.

Davidson & Co. (2007) – Personal Information of 192,000 individuals was stolen from the brokerage firm when hackers broke into a database server. In 2010, the Financial Industry Regulatory Authority fined Davidson & Co. \$375,000 in connection with the data breach, citing the brokerage firm’s failure to implement security measures.

Certegy Check Services (2007) – Nearly six million records containing Personal Information were stolen from Certegy, a check cashing verification service, by a senior database administrator of the company, who admitted to selling the stolen records to a direct marketer.

The costs of settling third-party class actions that often follow in the wake of data breaches at financial institutions is demonstrated by the October 27, 2009 announcement that the U.S. District Court Judge overseeing the California class action arising from The Ameritrade Holding Corporation breach of a database containing information of 6.2 million current and former customers had refused to approve a proposed settlement on the grounds that it was insufficient. The proposed settlement had reportedly provided for the cost of one year of anti-spam service for the victims as well as \$1.1 million in legal fees for the plaintiffs' lawyers. The data theft reportedly did not result in any identify theft, and though a database with Personal Information was hacked, the information was reportedly not taken. In December 2010, the court approved a new settlement that will reportedly cost the company between \$2.5 million and \$6.5 million.²⁵⁰ Similarly, the fine of \$375,000 imposed on Davidson & Co. by the Financial Industry Regulatory Authority noted above demonstrates that breached financial institutions are subject to large regulatory fines as well as third-party lawsuits.

Hacking of financial institutions raises not only concerns of large-scale theft of Personal Information, but also the specter of hackers deliberating wrecking havoc on global financial markets. Such concerns have reportedly led federal agencies such as the National Security Agency (NSA) and FBI to provide banks with intelligence on foreign hackers to help fend off cyber attacks.²⁵¹

f. Payment Processors

Payment processors of credit card transactions are a major target of malicious attacks, as a successful attack on their systems can yield large results for those whose goal is obtaining Personal Information for use in fraudulent financial transactions. Among the best known of these data breaches are:

Heartland Payment Systems (January 20, 2009) – The company, which processed 100 million credit card transactions per month, discovered that malicious software placed on Heartland's computer network had compromised card data that crossed the network.

RBS World Pay (December 2008) – The U.S. payment processing arm of the Royal Bank of Scotland Group announced that its computer system had been improperly accessed. Affected were prepaid cards including payroll cards and gift cards. Active fraud was reported on only 100 cards, with approximately 1.5 million cardholders affected by the

²⁵⁰ TD Ameritrade Holding Corp. – Form 10K – November 19, 2010.

²⁵¹ Anrea Shalal-Esa and Jim Finkle. *Exclusive: NSA helps banks battle hackers*, Reuters, October 26, 2011.

breach, and of that group 1.1 million people may have had their Social Security numbers affected.

The reported costs resulting from the Heartland breach demonstrate the potential size of exposures presented by data breaches of payment processors, who by the nature of their business have Personal Information of thousands (or millions) on their systems. In May 2009, Heartland disclosed it had spent or set aside more than \$12.6 million to cover legal costs and fines related to the data breach up to that date. A major portion of those costs was reportedly a fine imposed by MasterCard. Apparently one issue was whether Heartland responded appropriately after being warned of suspicious activity. This is separate and apart from settlements reached with the class of affected consumers, and settlements with other third parties.

Settlements reached by Heartland with the card brands represent an additional significant cost.. In December 2009, Heartland reportedly entered a settlement with American Express for \$3.6 million;²⁵² in January 2010, it settled with Visa for up to \$60 million;²⁵³ and in May 2010, it reportedly settled with MasterCard for \$41.4 million.²⁵⁴

A number of other financial institutions were reportedly affected by the Heartland data breach, including banks in 40 states. Many banks apparently had credit or debit cards they had issued compromised by the incident. One website published a list of over 150 institutions said to have publicly disclosed to their customers that they were victimized as a result of the Heartland breach. Heartland shareholder litigation was also commenced.

The Heartland breach demonstrates the wide range of third-party claims that may be asserted when there is a large breach resulting in unauthorized access of credit card numbers, as well as the significant first-party costs to which a company that has a large breach is subject.

g. Law Firms

Law firms are a repository of clients' confidential and Personal Information, and the Personal Information of claimants in litigations they handle, as well as their own employees' Personal Information. Thus, they are a significant potential source of inadvertent data breaches as well as a potential target of malicious ones.²⁵⁵ In addition, law firms that do a significant amount of business with companies in the healthcare industry may qualify as "business associates" of entities covered by HIPAA, and thus be subject to its breach notification requirements. Furthermore, law firms that perform large-scale document review and productions often use

²⁵² Robert McMillan, *Heartland Pays Amex \$3.6 Million Over 2008 Data Breach*, www.pcworld.com, December 17, 2009.

²⁵³ Grant Gross, *Heartland to Pay up to \$60 Million to Visa Over Breach*, www.pcworld.com, January 8, 2010.

²⁵⁴ Nancy Gohring, *Heartland, MasterCard Settle Over Data Breach*, www.pcworld.com, May 9, 2010.

²⁵⁵ See Dan Harper, *'Hactivists' and the Security of Law Firm Electronic Evidence*, *Chicago Lawyer Magazine*, October 2011; LWG Consulting, *Law Firms: The Next Cyber Attack Target?*, December 13, 2011.

outside vendors and Internet-based data storage systems. As this practice continues to grow, law firms increase their exposure to potential cyber attack as well as inadvertent data breaches involving their vendors as well as themselves.

Some examples are:

California law firm (December 2010) – An unknown number of consumer credit reports stored in the firm’s computer system were compromised when an unauthorized party obtained the computer system’s login information.

New York firm (Spring 2009) – A firm had its discarded files found in a dumpster, unshredded, containing Personal Information and medical records of claimants in old personal injury actions. The firm reportedly had retained a vendor to properly dispose of the files.

Texas law firm (November 2008) – A firm reported that a computer and used jump drive from its former offices were found and contained 627 names, many with their Social Security numbers, of employees of a plant that may have been involved in a lawsuit in the late 1990s.

Texas Law Firm (July 2008) – A firm had files containing Personal Information of the law firm’s clients, including financial records, Social Security numbers, and medical records, uncovered by sheriff’s deputies in a Houston dumpster.

h. Real Estate Agents

Real estate and rental agents and others involved in the sale or rental of properties maintain applications that contain financial information as well as other Personal Information of applicants, and thus are a source of data breaches that is often not fully considered. Some examples:

KC Realty (October 2010) – The owner of KC Realty (and two related financial services businesses) stole her own realty clients’ Personal Information to obtain 47 fraudulent loans totaling \$17.5 million.

In 2008, boxes containing loan applications, Social Security numbers and bank account information of residents were discovered in a model home abandoned by a bankrupt home developer in Arizona.

In late 2007 a realty company had computers that contained Personal Information, including Social Security numbers, of between 500 and 1,000 clients stolen in a burglary.

In early 2007, approximately 40 boxes of financial information maintained by a realty company, containing bank account numbers, Social Security numbers and photographs of driver's licenses, were found in a dumpster.

i. Employers of All Varieties

As illustrated above, many of the data breaches reported involved not the data of a company's customers, but rather of its own employees. Employers retain Personal Information data of their employees for a variety of reasons, including payroll and benefits. Breached information, in some cases, involved the data of *former* employees, illustrating the long-term hazard that may have prompted Massachusetts to require entities affected by their new regulations to limit the time period of the retention of data to only that which is necessary for their business operations. Compromised employee data also illustrates that virtually *any* type of institution that employs a staff, whether for-profit or not, is potentially at risk for a data breach.²⁵⁶ Among the recent examples demonstrating this risk is:

AMR Corp. (parent of American Airlines) (June 2010) – A computer hard drive containing Personal Information, including Social Security numbers and financial information, of about 79,000 retirees and former employees was stolen from the company's pension office.

j. Utilities

As cyber attacks on utilities demonstrate, data breaches are not limited to personal information. Tests conducted by the U.S. Department of Homeland Security, as well as actual attacks, demonstrate that cyber terrorists have the capability of disrupting, or even destroying, utilities such as electrical generation and transmission facilities, water treatment facilities, and facilities of the fossil fuel industry.²⁵⁷ Such attacks may result from what the industry refers to as an Advanced Persistent Threat (APT) – that is, a group, such as a foreign government, with both the capability and the intent of targeting a specific entity with a cyber attack.²⁵⁸

In the spring of 2009, cyber spies reportedly penetrated the nation's electrical grid.²⁵⁹ This incident highlighted that utility companies are a target, with resultant effect on those they service. The sequelae of the East Coast blackout of 2004 demonstrated the effect and scope of potential business interruption and related losses that can be incurred as a result of a utility

²⁵⁶ See *Allison v. Aetna, Inc.*, filed in June 2009 in the U.S. District Court for the District of Pennsylvania. The suit was filed on behalf of former, current and prospective employees who applied for jobs through the company's website, whose security was breached, allegedly exposing the Personal Information of at least 65,000 current and former employees whose applications dated back several years.

²⁵⁷ See, e.g., Phil Windley, *Blowing up generators remotely*, ZDNet.com, September 28, 2007.

²⁵⁸ See *Under Cyberthreat: Defense Contractors*, Bloomberg Businessweek, July 9, 2009.

²⁵⁹ S. Gorman, *Electricity Grid in U.S. Penetrated by Spies*, The Wall Street Journal, April 8, 2009, page A1.

failure. As the blackout demonstrated, businesses dependent on refrigeration are especially vulnerable to large losses resulting from electrical failures with resultant first-party and third-party claims.

In February 2011 it was reported that Chinese hackers had infiltrated the computer systems of five multinational oil and gas companies, in an attack dubbed “Night Dragon.” Security researchers stated that the purpose of the attack appeared to be corporate espionage, as the focus appeared to be on oil and gas field production systems as well as financial documents.²⁶⁰

Whether the aim is to steal secrets or to disrupt facilities, utilities are likely to continue to be a target for cyber criminals.²⁶¹

k. Defense Industry/Military Industrial Complex

Companies and agencies comprising the U.S. Military Industrial Complex are a target of cyber attacks aimed at access to confidential information other than Personal Information, and perhaps at business disruption. An indication of that is reports that the Defense Department detected 360 million attempts to penetrate its networks in 2008, up from six million in 2006. In the Spring of 2008, there was reportedly a breach of one of the Pentagon’s Joint Strike Fighters weapons program.²⁶² Reportedly similar incidents resulted in the breach of the Air Force’s air-traffic control system.²⁶³ One report of a U.S. Department of Defense breach identifies a vulnerability faced by all companies: thumb drives.²⁶⁴

The Defense Department has created a new military command to defend U.S. military computer networks against cyber attacks. The so-called cyber-command will also be capable of launching attacks against enemy computer networks. General Keith B. Alexander, director of the National Security Agency, was nominated by President Obama in October 2009 to head the new command, and was confirmed by the U.S. Senate on May 7, 2010.²⁶⁵ The Defense Department reported on November 3, 2010 that the U.S. Cyber Command had reached “full operational capacity.”²⁶⁶

²⁶⁰ John Markoff, *Hackers Breach Tech Systems of Oil Companies*, The New York Times, February 10, 2011.

²⁶¹ See section above: Cyber Attacks with Physical Effects or Business Disruption as Focus.

²⁶² S. Gorman and Y. J. Dreazon, *Obama Set to Create ‘Cyber Czar’ Position*, The Wall Street Journal, May 29, 2009, page A4.

²⁶³ S. Gorman, A. Cole, Y. Dreazen, *Computer Spies Breach Fighter-Jet Project*, The Wall Street Journal, April 21, 2009, page A1.

²⁶⁴ Deloitte, *The Sixth Annual Global Security Survey* at p. 32 (reporting media speculation that “a recent worm attack, acknowledged by the U.S. Department of Defense (DoD) may have been linked to thumb drives after the DoD subsequently banned them”).

²⁶⁵ Ellen Nakashima, *Gen. Keith Alexander confirmed to head cyber-command*, The Washington Post, May 11, 2010.

²⁶⁶ See <http://www.defense.gov/releases/release.aspx?releaseid=14030>.

Private companies involved in development of products for the Defense Department are also targets, with resultant costs including contractual penalties, business interruption and reputational damage. This was demonstrated recently by the May 2011 cyber attack on Lockheed Martin, a major defense contractor holding sensitive information (although the company reported its secrets remained safe). This attack reportedly may be tied to an earlier hacking attack on the RSA security division of EMC Corporation that reportedly may have comprised security products RSA supplied to companies in the military industry and to other large corporations.²⁶⁷

Similarly, think tanks have also recently been targeted. Over the 2011 December holiday, Stratfor, a security think tank, was targeted by the hacking group Anonymous (sometimes referred to as “hactivists”). Confidential customer information was reportedly accessed, as well as individuals’ credit card numbers which Anonymous reportedly used to make “donations” to charities.²⁶⁸ The attack demonstrates that financial gain need not be the focus of a cyber attack for Personal Information to be involved, as well as demonstrating the challenges for even sophisticated security entities to secure their systems against cyber attacks.

The U.S. defense industry is not alone in being targeted. In the fall of 2011, the Japanese defense industry also reported a cyber attack.²⁶⁹ Such attacks have illustrated the global risk and need for international cooperation.²⁷⁰

As the recently retired U.S. Deputy Secretary of Defense put it on September 28, 2011:

In a development of extraordinary importance, cyber technologies now exist that are capable of destroying critical networks, causing physical damage, and altering the performance of key systems. In the twenty-first century, bits and bytes are as threatening as bullets and bombs.”²⁷¹

Cyber attacks on government facilities or critical infrastructures industries raise new and complex issues of national security, public policy, and the necessary and appropriate degree of cooperation between the government and the private sector. U.S. policymakers are struggling to address these issues.

²⁶⁷ Christopher Drew and John Markoff, *Data Breach at Security Firm Linked to Attack on Lockheed*, The New York Times, May 27, 2011.

²⁶⁸ See, e.g., Sean Ludwing, *10 things you need to know about Anonymous’ Stratfor hack*, Venture Beat, December 28, 2011. Oliva Katrandjian, *Hacking Group ‘Anonymous’*, ABC World News, December 26, 2011.

²⁶⁹ James Simpson *Defense Industry Hacking Cases Likely Linked*, Japan Security Watch, New Pacific Institute, October 16, 2011; *Mitsubishi Heavy Industries Hacked: Japan Defense Industry’s First Cyberattack*, Reuters, September 19, 2011.

²⁷⁰ See section above: *Cyber Attacks with Physical Effects or Business Disruption as Focus*.

²⁷¹ William J. Lynn III, *The Pentagon’s Cyberstrategy, One Year Later*, Foreign Affairs, September 28, 2011.

I. Other Governmental Entities

Federal, local, and state entities aggregate vast amounts of sensitive information, and they can be as susceptible to breach of such data as any private entity. Some recent examples include:

U.S. Chamber of Commerce (December 2011) – A group of hackers in China reportedly breached the U.S. Chamber of Commerce computer system and gained access to information stored in its system, including information about its members.

Massachusetts Executive Office of Labor and Workforce Development (May 2011) – Personal Information, including Social Security numbers, of approximately 210,000 people was compromised by a computer virus infecting various computers at the Department of Unemployment Assistance, the Department of Career Services, and multiple One Stop Career Centers.

Social Security Administration (April 2011) – the Social Security numbers of approximately 64,000 living people were made available on the Social Security Administration’s Death Master File.

Texas Comptroller’s Office (April 2011) – Personal Information, including Social Security numbers, of 3.5 million Texans was found to be accessible on a public server. In May 2011, two class action lawsuits were filed against the Texas Comptroller’s Office.

Government entities and political parties also face the threat of cyber attacks from politically motivated groups as well as financially motivated criminals, as demonstrated by recent threats and attacks of the “hactivist” group Anonymous, and concerns of groups involved in upcoming Presidential caucuses.²⁷²

m. Vendors

Breaches by companies’ third-party service providers such as outsourcers, contractors, consultants, and business partners were reported by 44% of the entities responding to a study of data breaches. That same study reported that per victim costs are \$52 higher for third-party “flubs” than if the breach is caused internally at the company whose data was compromised.²⁷³

Outsourcing of services is increasingly common, and often involves transfer of or allowing access to Personal Information from a company to its vendor, such as IT, payroll, accounting, pension and other financial services.

²⁷² Ryan J. Foley, *Iowa GOP worried by Hacker threat to caucus vote*, Associated Press, December 19, 2011.

²⁷³ Ponemon Study, *supra*.

Entities that provide vendor services to other companies are a potential source of data breach risk for their clients. Particularly if they do not institute their own data protection procedures in compliance with applicable regulations or industry standards, the data they store of their clients' employees or customers is subject to either loss or malicious theft, including from an insider at the vendor itself. Even when data protection security standards are in place, vendors with large amounts of personal or other sensitive information can make attractive targets for hackers.

Some examples are:

Vacationland Vendors, Inc. (September 2011) – A third-party supplier of arcade equipment and vending machines to an assortment of businesses announced that information concerning up to 40,000 credit or debit cards used in its machines was stolen in a breach of the company's card processing system.

Epsilon (April 2011) – A vendor that provides consulting, marketing data, technology and agency services to major retailers announced that the customer data of many of its more than 2,500 corporate clients, was exposed by an unauthorized entry into its email system.

Unnamed vendor (December 2010) – A hacker targeted a vendor maintaining a mailing list for American Honda Motor Company and stole the names, email addresses, and vehicle identification numbers of nearly five million Honda and Acura owners.

University of Utah/Perpetual Storage (June 2008) – A vendor that stored data for the university allegedly lost data containing Personal Information on 1.7 million patients of the university hospital and clinics when backup storage tapes were stolen from the personal vehicle of the vendor's employee.²⁷⁴

University of Connecticut Foundation/Convio (November 2007) – A vendor that processed online gift transactions for a variety of institutions suffered a security breach, affecting the data of 92 of its clients.

Med Data (September 2006) – The manager of a billing company for a hospital in Washington State stole patients' credit card numbers.

Morris, Davis & Chan (September 2006) – An auditor had a laptop stolen containing personal information of employees of its client, a law firm.

²⁷⁴ The incident is the subject of insurance coverage litigation venued in the United States District Court for the District of Utah. The vendor's liability insurer brought a declaratory judgment action in which it disputes coverage under both a commercial package policy and a general liability policy. *Colorado Cas. Ins. Co. v. Perpetual Storage Inc.*, Case No. 2:10-cv-00316-BCW (D. Utah).

InstantDx (July 2006) – An online prescription provider retained personal data of patients of a Georgetown hospital, which used the company’s e-service. A computer consultant discovered that he was able to easily access the private data online.

Vendors who lose or are the subject of hacking of customer information that includes Personal Information of, for example, their customers’ employees can be subject to claims by those whose information is lost, as well as by their client companies.²⁷⁵

3. Insurance Company Exposures

a. Exposure of Companies in the Insurance Industry as Entities Subject to Data Breaches

While insurers generally focus on the exposures of their insureds, they are themselves in an industry in which companies have potential exposure to data breaches.

Insurance industry companies have the same vulnerabilities to data breach as other institutions. Some may even have an elevated risk due to their heavy dependence on computer systems and the nature of the information stored on their systems.

First, at risk is their own employee information. As large-scale employers, often of employees residing in many different states – including Massachusetts with its rigorous data security requirements – insurers, reinsurers, brokers and companies servicing the insurance industry are subject to breach of their own employees’ Personal Information, including payroll, personnel, pension, workers’ compensation and disability claim information.

Second, at risk is the Personal Information insurers have of insureds, claimants and beneficiaries. Liability insurers often have claimant information, ranging from medical records and financial documents to claimants identified by name and Social Security number which, if lost or improperly accessed, would be a data breach of Personal Information. Personal lines and life and health insurers may maintain Personal Information of policyholders and of beneficiaries, which are also subject to data breaches. Such Personal Information may remain stored by

²⁷⁵ See, e.g., *Caudle v. Towers, Perrin, Forster & Crosby, Inc.*, 580 F. Supp. 2d 273 (S.D.N.Y. 2008). In that case, the court dismissed claims for negligence and breach of fiduciary duty brought by an employee against his employer’s pension consultant whose laptop containing Personal Information of employees was stolen; the employee sought on behalf of himself and others credit monitoring costs. The court dismissed the negligence claim in the absence of evidence that the information had been accessed or used. It also dismissed the claim for breach of fiduciary duties, again on the ground that the plaintiff had not shown he had suffered any damages. The court did allow the claim for breach of contract to proceed to allow discovery on the issue of whether the employee was a third-party beneficiary of the contract between his employer and the vendor under the terms of the contract. See also *Ruiz v. Gap, Inc.* 622 F. Supp.2d 908 (N.D. Cal. 2009) (in which plaintiffs sued a company’s vendor for losing their Personal Information when a laptop was stolen containing information with job applications; the court dismissed the claims for lack of requisite appreciable harm in light of the fact that the plaintiff had not been a victim of identity theft but rather was claiming increased risk of future identity theft and seeking credit monitoring costs), *aff’d*, 380 F. App. 689 (9th Cir. 2010) (holding that under California law, a plaintiff must have either prior possession or a vested legal interest in money or property lost in order to claim restitution).

EDWARDS WILDMAN PALMER LLP

insurers, reinsurers, brokers, and third-party administrators as well as vendors of such entities, either in paper or electronic form, for decades.

Insurers are also subject to extensive state and federal regulation that includes requirements for safeguarding Personal Information and reporting data breaches, as well as to common law standards for protecting confidential information.²⁷⁶

The Departments of Insurance of several states have issued bulletins and regulations requiring insurers doing business in their states to send data breach notifications to the departments of insurance when an insurer has suffered a data breach. For example, Ohio Insurance Bulletin 2009-12 requires insurers to provide notice to the Ohio Department of Insurance of loss of control of policyholder information within 15 calendar days after discovery of the loss of control if it involves more than 250 Ohio residents. Pursuant to Chapter 11 of Rhode Island Insurance Regulation 107, licensees of the Rhode Island Department of Business Regulation, which includes insurance companies, must notify the department of a data breach in the most expedient time possible and without unreasonable delay. Similarly, the Wisconsin Office of the Commissioner of Insurance, under a bulletin dated December 4, 2006, requires that insurers notify the office no later than 10 days after it has become aware of unauthorized access to the Personal Information of insureds. The Connecticut Department of Insurance issued Bulletin IC-25 on August 18, 2010 to require all entities doing business in Connecticut that are licensed by or registered with the Department to notify the Department of any information security incident. Notice must be provided as soon as the incident is identified, but no later than five calendar days after the incident is identified. The Connecticut Bulletin lists numerous facts that must be disclosed in the notification to the Department of Insurance as they are known at the time, including details about the incident and remedial actions taken. Notice must also contain a draft of the notice the licensee or registrant intends to send to Connecticut residents. The Bulletin also imposes a requirement on the licensee or registrant to report incidents involving a vendor or business associate.²⁷⁷

Insurers are also subject to federal and state regulations of Personal Information that are not specifically directed at the insurance industry, but apply to companies in the industries as entities that obtain and maintain Personal Information. Thus, for example, the broad-ranging Massachusetts Regulation discussed above affects any entity that has Personal Information of a

²⁷⁶ In *Daly v. Metropolitan Life Ins. Co.*, 4 Misc. 3d 887, 782 N.Y.S. 2d 530 (2004), a New York state court denied a motion to dismiss claims brought by a life insurance applicant against a life insurer arising from the purported theft of her personal information by a janitor who cleaned the insurer's premises and which resulted in fraudulent use of her personal information to create credit accounts. The court noted that after completing her application, the applicant had received a Privacy Notice from the insurer detailing the company's privacy policy and stating that confidential information would be safeguarded. The court found that the gravamen of the plaintiff's claim was that in order to obtain a life insurance policy the plaintiff had to provide sensitive personal information and the insurer represented that information would be protected and remain confidential. Thus, the court found that the insurer had a common law duty to protect the confidential personal information provided by the applicant, and in light of questions of fact concerning precautions taken by the insurer to safeguard that information it denied summary judgment of claims at that juncture.

²⁷⁷ The Connecticut Bulletin is available at <http://www.ct.gov/cid/cwp/view.asp?a=1255&q=254256&cidNav=487751>.

Massachusetts resident, and thus is likely to affect a significant number of insurers. It will technically apply to liability insurers with Personal Information of Massachusetts claimants and to life insurers that have Personal Information of non-policyholder beneficiaries, as well as to those with employees or insureds who are Massachusetts residents.

Accordingly, in addition to the exposures insurers face as the issuers of policies that may cover the costs of data breach incurred by their insureds and claims asserted against insureds arising from data breaches, insurers and other entities in the insurance industry have their own risk of data breaches.

b. Potential Insurance Coverage for Data Breaches

The increasing range of costs incurred by entities that sustain a breach and the third-party claims against them have given rise to efforts by entities that have sustained a breach to seek coverage for those costs and claims. Specialty insurance products have been developed to specifically address data breach risks, although not all address the full scope of costs and claims. Moreover, entities that sustain a breach that have not purchased policies directed at providing data breach coverage often look with varying success and failure to the more traditional types of policies they have in place for coverage of at least some of the costs, defense and indemnity payments they incur.

A number of different types of insurance policies have the potential to be implicated in the event of a data breach – or at least to be subject to a request for defense and/or indemnity – depending on factors such as the type of breach, the relationship of the parties, the nature of the information in issue (Personal Information, Intellectual Property), the type of policy in issue and, if for third-party liability, the allegations asserted and the type of damages in issue. As in all requests for coverage, the issue of coverage turns on policy terms, including both grants of coverage and exclusions, as well as on the specifics of the claim.

As the risk of data breaches becomes increasingly recognized, policy exclusions and definitions are being added and tightened to reduce the exposure of policies not intended to apply to data breach risks, and sublimits for some types of costs are often added even to those policies expressly directed at insuring the risk of data breach. Many insurers impose application procedures directed at identifying the risk of data breach and the security procedures of the applicant entities, and some impose risk management conditions before agreeing to issue a policy that provides coverage for these types of claims.

Some of the issues that may be presented by a claim for coverage are identified below, although of course the issues can vary depending on the claim and the policy wording.

(i) Cyber Risk/Data Breach/Privacy/Network Security Policies

A growing number of insurers are offering policies specially tailored to provide coverage for a variety of cyber risks, ranging from breaches of Personal Information, to cyber extortion, to

business interruption arising from cyber attacks. Coverage has even been developed for liability associated with social media such as posting of a defamatory comment on a blog. Some of these policies are industry-specific, such as cyber risk insurance designed for technology companies, restaurants, healthcare entities, or financial institutions. In the current market, coverages are often expanded and new coverages developed, including express coverage for the Payment Card Industry (PCI) fines and penalties that are often associated with breaches of Personal Information involving credit card numbers. As data protection regulations and statutes, with concomitant breach response requirements, continue to be enacted and expanded in the U.S., E.U, and elsewhere, the market for such specialty products is expanding and new products are likely to be developed.²⁷⁸

Policies designed to provide data breach coverage do not necessarily restrict themselves to electronic breaches of statutorily defined Personal Information, but may also broadly encompass coverage for breach of privacy costs and claims arising from other types of data breach including loss or theft of Personal Information contained in paper records and information that, while not itself Personal Information, can be used to obtain Personal Information. In addition to providing insurance coverage, some insurers offer data breach prevention services to their clients; one insurer announced that it would be pairing its healthcare-related cyber liability coverage with a third-party email encryption service.

Some of these policies have both first and third party coverages. First-party coverages in such policies are generally designed to pay or reimburse an insured that has sustained a breach for its own costs incurred in addressing a breach such as notification costs, although some such policies limit coverage of notification costs to situations in which the insured is legally obligated to provide notice of data breach under state or federal statutes or to a maximum number of individuals. Policies directed at providing coverage for data breaches may also provide some coverage for costs directed at mitigating loss or reducing the likelihood of third-party claims such as legal advice as to the company's notice obligations, credit monitoring offered to those whose Personal Information is compromised, and forensic investigation as to the cause of the breach. Some policies offer first-party coverage for business interruption losses related to data breaches, even in the absence of physical damage to tangible property. Liability coverages for defense costs and damages arising from a claim by a third party of damages arising from a data breach are also generally the subject of express coverages under such policies. Some cyber risk policies now also integrate coverage for online media liability.

However, even policies directed at providing coverage for data breaches of Personal Information vary in the scope of coverages provided and often have sublimits for certain types of costs or damages, and exclusions for others. Issues can arise as to whether there is coverage of costs incurred by an insured that are not legally required but are undertaken to preserve an insured company's reputation or reduce the likelihood of a third-party claim; of contractual indemnity

²⁷⁸ See, e.g., *Data protection measures could increase demand for cyber risk products*, Post Magazine, December 16, 2011; *Cyber risks and data privacy market set for strong 2012 growth*, Insurance Insider, December 12, 2011;

obligations; of contractual fines and penalties as well as fines and penalties imposed by regulatory authorities; of breaches due to insured/employee dishonesty; of business interruption loss; and of other types of claims or costs. The terms of these new policies are largely untested by the courts, and their terms, conditions and exclusions are still in flux.

(ii) Property Policies – First-Party

First-party property policies, which usually cover physical damage to real and personal property and may (depending on their terms) also provide coverage for resulting business interruption, may be scrutinized by insureds looking for potential insurance coverage, particularly those who sustain not only a data breach, but also business interruption losses, or costs for replacement of a computer system or data storage unit as a result of a breach.

However, such claims generally fail in the absence of some indication of physical damage to the computer system involved. Such policies generally cover “direct physical loss or damage” to insured property caused by a covered cause of loss. “Physical” is generally construed to mean “tangible.”²⁷⁹ Case law generally maintains that electronic data is not tangible property.²⁸⁰

Further, policy exclusions often specifically exclude or limit coverage of electronic data and other “valuable papers and records.” Business interruption coverage is generally required to result from damage to or destruction of property caused by a loss otherwise covered under the policy, and thus if there is no physical loss or damage to tangible property in a data breach, the resultant business interruption losses are also generally not covered under a traditional property policy.

Non-coverage of a claim under a policy, though, cannot always be assumed. If a computer becomes unusable due to the installation of malware, a policyholder may be able to seek recovery under a coverage for loss of use of tangible property that is not physically injured.²⁸¹ There can also be claims involving destruction or corruption of electronic data on the system of the insured due to viruses which may be covered under the limited electronic data additional

²⁷⁹ See, e.g., *Florists’ Mut. Insurance Co. v. Ludy Greenhouse Mfg. Corp.*, 521 F. Supp.2d 661, 680 (S.D. Ohio 2007); *Philadelphia Parking Authority v. Federal Insurance Co.*, 385 F. Supp.2d 280, 288 (S.D.N.Y. 2005).

²⁸⁰ See, e.g., *Ward General Services, Inc. v. Employers Fire Ins. Co.*, 114 Cal.App.4th 548, 556-57 (Cal.App. 4 Dist. 2003); *Southeast Mental Healthcare Center, Inc. v. Pacific Insurance Company, LTD*, 439 F.Supp.2d 831, 838-839 (W.D. Tenn. 2006); *America Online, Inc. v. St. Paul Mercury Ins. Co.*, 347 F.3d 89, 93-98 (4th Cir.2003); *State Auto Property & Cas. Ins. Co. v. Midwest Computers & More*, 147 F.Supp.2d 1113 (W.D.Okla. 2001). Courts reaching a different conclusion have done so where the data is permanently lost to its owner, not merely improperly accessed. See *Computer Corner, Inc. v. Fireman’s Fund Ins. Co.*, 46 P.3d 1264 (N.M. 2002) (holding that loss of the pre-existing electronic data was tangible property damage covered by CGL policy where computer store repairing customer’s computer permanently lost all the data); *American Guar. & Liab. Ins. Co. v. Ingram Micro, Inc.*, 2000 WL 726789, 2000 U.S. Dist. LEXIS 7299 (D. Ariz. Apr. 18, 2000) (holding that computer data permanently lost during a power outage constituted “direct physical loss or damage from any cause” covered by first-party insurance policy); *NMS Services Inc. v. Hartford*, 62 Fed.Appx. 511 (4th Cir. 2003) (characterizing the erasure of vital computer files and databases as direct physical loss or damage to property for purposes of business income coverage).

²⁸¹ See, e.g., *Eyeblaster, Inc. v. Federal Ins. Co.*, 613 F.3d 797 (8th Cir. 2010).

coverage provided by some property policy forms.²⁸² Further, there can be endorsements and other manuscript provisions added to more traditional business property forms that expressly provide some additional limited coverage for impairment of data systems and papers and other losses implicated in a data breach claim. Should there be potential coverage of any portion of a loss under a property policy, loss mitigation provisions may also be targeted by policyholders as a basis for requests for coverage of loss mitigation costs.

(iii) Fidelity Insurance – Employee Crime

In the 1990 film *Ghost*, one of the characters, who works at a financial institution, sets up a dummy account to facilitate a money-laundering scheme. In the event of a hypothetical real-world scenario where an insider steals customer account data in order to siphon money out of customers' accounts – and in the absence of a Patrick Swayze to change the password and thwart the crime – the financial institution might be able to bring a claim under its Fidelity and Crime insurance policy. Such policies generally protect organizations from the loss of money, securities, or inventory resulting from employee crime. “Common Fidelity/Crime insurance claims allege employee dishonesty, embezzlement, forgery, robbery, safe burglary, computer fraud, wire transfer fraud, counterfeiting, and other criminal acts.”²⁸³

Many data breaches involve theft and other criminal conduct by employees, *e.g.*, theft of laptops or other computer equipment containing Personal Information or other confidential data. Thus, depending on its terms and exclusions, the company's fidelity insurance may be triggered. Some fidelity or crime insurance policies may expressly provide for computer crime coverage in the form of a computer fraud endorsement, while others may contain exclusions that limit or preclude such coverage.

(iv) CGL – Third-Party Claims

An insured entity subjected to a lawsuit in connection with a data breach it suffers may tender the defense of that suit under its commercial general liability policy. While privacy and data security are developing areas of the law, there are a few judicial decisions indicating the likely issues on which a coverage dispute will focus when a claim for coverage is made under a CGL policy.

²⁸² See, *e.g.*, *Lambrecht & Assocs. Ins. v. State Farm Lloyds*, 119 S.W.3d 16 (Tex. App. 2003) (holding that a property policy covered loss of business income due to damage to software and electronic data by a virus, where the section of the policy defining coverage for loss of income included “electronic media and records,” defined to include electronically stored data); see also *Southeast Mental Health Center, Inc. v. Pacific Ins. Co., Ltd.*, 439 F.Supp.2d 831,837-39 (W.D. Tenn. 2006) (finding corruption of a commercial insured's pharmacy computer after a storm and power outage constituted “direct physical loss of or damage to property” under business interruption policy).

²⁸³ Hossein Bidgoli, *Handbook of Information Security*, 820 (John Wiley and Sons, 2006).

(1) Coverage A

Coverage A of a CGL policy typically provides that “we will pay those sums that the insured becomes legally obligated to pay as damages because of ‘bodily injury’ or ‘property damage’ to which this insurance applies.” “Property damage” is typically defined as “physical injury to tangible property, including all resulting loss of use of that property,” and “loss of use of tangible property that is not physically injured.”²⁸⁴

Generally in data breach cases, the focus of analysis as to whether there is coverage, or at least sufficient allegations to trigger a duty to defend, is on the “property damage” requirement of Coverage A. Because of the required component of “tangible property,” it is usually considered unlikely that lawsuits related to a typical breach of electronic data security would be covered under Coverage A. As in the first-party property policy context, case law generally maintains that electronic data is not tangible property.²⁸⁵ Additionally, ISO’s 2004 form and other CGL forms include in the definition of “property damage” the provision that “for the purpose of this insurance, electronic data is not tangible property.”²⁸⁶

In addition, the 2004 ISO form includes an Electronic Data Exclusion, according to which “this insurance does not apply to... damages arising out of the loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data.” Under policies containing such an exclusion, for there to be any coverage there would need to be losses caused by physical injury to, or the loss of use of, “tangible property,” which must be something other than electronic data. However, there may be data breaches involving data other than electronic data for which insureds may be able to satisfy the “tangible property” requirement as well as the “occurrence” requirement, and demonstrate either physical injury to that property or loss of use of the property containing the data.

Further, while analyses of whether Coverage A applies have focused on the property damage aspect of that Coverage Part, Coverage A also applies to “bodily injury.” The recent spate of consumer third-party claims has often included an emotional distress component. Thus, if a policy or governing law defines “bodily injury” as including emotional distress even when there is no physical injury, there potentially could be a claim for coverage for that aspect of the alleged

²⁸⁴ This is standard policy language in recent ISO form policies (see CG 00 01 12 04). While there is variance in language among different insurers’ CGL policies, the ISO language is in widespread use and there are judicial decisions dealing directly with ISO wordings.

²⁸⁵ *But see, e.g., Eyeblander, Inc. v. Federal Ins. Co.*, 613 F.3d 797, 801-02 (8th Cir. 2010) (underlying allegations of loss of use of a computer – *e.g.*, that the computer “froze,” was “taken over and could not operate,” and was otherwise “no longer usable” due to software installed by the insured – found sufficient to satisfy the “loss of use of tangible property that is not physically injured” prong of the definition of “property damage”).

²⁸⁶ The ISO definition of “property damage” also defines “electronic data” for purposes of applying the policy: “As used in this definition, electronic data means information, facts or programs stored as or on, created or used on, transmitted to or from computer software, including systems and applications software, hard or floppy disks, CD-ROMS, tapes, drives, cells, data processing devices or any other media which are used with electronically controlled equipment.”

damages. However, while the “tangible property” barrier would not apply to such a claim, the insured would still have to demonstrate that the “bodily injury” was caused by an “occurrence” and that the Electronic Data Exclusion did not apply, and circumvent any other provisions that may be added by an insurer to its policy to preclude coverage of data breach claims. The potential for coverage may be more likely for data breaches directly causing demonstrable bodily injury, such as those involving computer-controlled medical equipment that impact medical care of individuals, rather than for the typical electronic data breach involving Personal Information.

(2) Coverage B

Attempts at seeking coverage, or at least obtaining a defense, under CGL policies have been asserted under Coverage B, Personal and Advertising Injury. Results have varied depending on jurisdiction and claim.

Personal and Advertising Injury coverage under Coverage B is limited to injuries arising out of certain enumerated offenses. Standard Coverage B coverage provides: “we will pay those sums that the insured becomes legally obligated to pay as damages because of ‘*personal and advertising injury*’ to which this insurance applies,” and the policy’s definition of personal and advertising injury generally lists the enumerated offenses for which coverage is provided. Among those enumerated offenses is typically “injury ... arising out of ... oral or written publication, in any manner, of material that violates a person’s right of privacy.” This is the offense that is often alleged to apply when a claim for coverage for a data breach is made.

To successfully tender a data breach claim under Coverage B, then, an insured would have to demonstrate, among other things, at least a potential that the data breach in issue constituted a “publication” that violated the data owner’s “right of privacy.” The standard ISO insurance form does not define the terms “publication” or “right of privacy.” Courts ruling on the applicability of Coverage B to privacy claims have found some types of personal data, but not others, to be within the data owner’s “right of privacy,” and the result can vary depending on the information and the jurisdiction’s law that applies. Thus, some courts have found privacy rights implicated for purposes of Coverage B where the issue was improper access and use of certain types of information that are statutorily protected, such as access and use of credit reports in violation of the Fair Credit Reporting Act (FCRA expressly states that it is intended to protect consumers’ right to privacy).²⁸⁷ Similarly, the personal data at issue in data breach scenarios is sometimes also protected by statutes designed to keep that data private. However, to the extent that the right

²⁸⁷ See *Pietras v. Sentry Ins. Co.*, 2007 WL 715759, 2007 U.S. Dist. LEXIS 67013 (N.D. Ill. 2007) (holding, under Illinois law, that the insurer had a duty to provide a defense); *American Family Mutual Ins. Co. v. C.M.A. Mortgage, Inc.*, 2008 WL 906230 (S.D. Ind. 2008) (holding under Indiana law that a claim involving improper use of credit reports in violation of FCRA states a potentially covered claim and thus triggers the insurer’s duty to defend) (*order rescinded in part due to docketing error*, 2008 WL 5069825); *Zurich American Ins. Co. v. Fieldstone Mortgage Co.*, 2007 WL 3268460 (Md. Dist. Ct. 2007) (holding, under Maryland law, that a FCRA claim based upon improper access and use of others’ credit information triggered a duty to defend).

to privacy is based on a statute, there may also be exclusions that serve to preclude coverage.²⁸⁸ Moreover, to the extent that a claim is based on a common law or constitutional right to privacy, under some states' law, only information that is of an embarrassing nature and published under egregious circumstances is considered to be in violation of a right to privacy.²⁸⁹

Even apart from the content of the information involved, the application of the "publication" requirement of Coverage B presents a significant hurdle in data breach cases, particularly those involving theft of information from the breached entity.. Decisions in some jurisdictions have found there to be sufficient issue of publication under some fact situations to at least trigger a duty to defend in situations that, among other things, have involved insured's alleged distribution of the personal information in issue; however, others have held there to be no coverage as a matter of law. Thus, for example, in Fair Credit Reporting Act cases, several courts took a broad view of "publication," and found that publication can occur when information is revealed by the insured to others, including the owner of the information. One court noted that "of the circuits to examine 'publication' in the context of an 'advertising injury' provision, the majority have found that the publication need not be to a third party,"²⁹⁰ and relying on a dictionary, found "publication" to mean "to produce or release for distribution."²⁹¹ In contrast, courts in other jurisdictions analyzing the application of Coverage B to a violation of FACTA reached a different conclusion with regard to "publication" on the grounds that it is not publication where credit card information is improperly printed in full, but is provided only to the cardholder and thus not "in any way made generally known, announced publicly, disseminated to the public, or

²⁸⁸ As mentioned below, to the extent *statutes* create a "right of privacy" in the type of personal information in issue, CGL policies typically also include an exclusion applicable to Coverage B for Violation of Information Law, that may preclude coverage for an claims for violation of such a statute.

²⁸⁹ See, e.g., *Allstate Ins. Co. v. Ginsberg*, 863 So.2d 156 (Fl. 2003) (finding absence of personal injury coverage because underlying claims did not allege common law violation of privacy); *Lextron, Inc. v. Travelers Cas. and Sur. Co. of America*, 267 F.Supp.2d 1041, 1047 (D. Colo. 2003) (looking to the Restatement (Second) of Torts for guidance); *A & B Ingredients, Inc. v. Hartford Fire Ins. Co.*, No. 08-6264, 2010 WL 5094419 (D. N.J. Dec. 8, 2010) (finding absence of personal and advertising injury coverage on the basis of a broad statutory exclusion and a finding that the jurisdiction in which the underlying claims arose apparently did not recognize common law privacy violations in that context); *Ananda Church of Self Realization v. Everest Nat. Ins. Co.*, No. C038570, 2003 WL 205144, 2003 Ca. App.Unpub. LEXIS 1095 (Cal. Ct. App. Jan. 31, 2003) (unpublished) (finding absence of Coverage B coverage, in part, on the basis that the type of information at issue, while confidential, were not facts that "the average person would find offensive or objectionable"); *Ruiz v. Gap, Inc.*, 540 F.Supp.2d 1121 (N.D. Cal. 2008), *aff'd*, 380 Fed.Appx. 689 (9th Cir. 2010) (holding that the employer's possible negligence (*i.e.*, in allowing the computers containing unencrypted personal information of job applicants to be stolen) did *not* rise to the level of egregiousness required). See also *State Farm Fire and Cas. Co. v. National Research Center for College and University Admissions*, 445 F.3d 1100, 1103 (8th Cir. 2006) (deciding under Missouri law and defining "privacy" as "isolation, seclusion, or freedom from unauthorized oversight or observation.")

²⁹⁰ See *Zurich v. Fieldstone*, *supra*, 2007 WL 3268460 at *5; see also, e.g. *Park Univ. Enterprises, Inc. v. American Cas. Co. of Reading*, 442 F.3d 1239, 1248-49, 1250 (10th Cir. 2006) (applying Kansas law and holding that violation of a law prohibiting unsolicited fax advertisements violated "a species of privacy interest"; that it is reasonable to define publication as "making something generally known" and faxing advertisements is to effectively "publish;" and that there was therefore a duty to defend).

²⁹¹ *Id.* See also *LensCrafters, Inc. v. Liberty Mut. Fire Ins. Co.*, No. C-04-1001, 2005 WL 146896 (N.D. Cal. Jan. 20, 2005) (involving alleged disclosure of private medical information); *Moore v. Hudson Ins. Co.*, No. B189810, 2007 WL 172119, at *6 (Cal. Ct. App. Jan. 24, 2007) (unpublished) (discussing scope of dissemination required).

EDWARDS WILDMAN PALMER LLP

released for distribution.”²⁹² However, in a case construing “publication” in the context of an employer subjecting his employee to audio surveillance without informing the employee in violation of the Wiretapping and Electronic Surveillance Act, the surveillance was found to constitute “publication.”²⁹³

Overall, the limited case law and legal authorities on the issue indicates that “publication” within the context of Coverage B requires that the insured have affirmatively disseminated the information in issue to at least one other person, rather than have that information stolen from it, for there to be any potential for the “publication” prong of Coverage B to apply.

Additional issues include whether there are any covered “damages” to which the insurance applies.

Thus, in the event of a request for coverage under Coverage B of a third-party claim based upon improper access to Personal Information due to a data breach, the focus is likely to be whether there was a violation of the data owner’s “right of privacy,” whether there was “publication” by the insured, whether covered “damages” are sought, and which jurisdiction’s law applies.

Variations in Coverage B policy wording can also affect whether a court is likely to find coverage for a data breach under Coverage B. In a case involving claims brought under the Electronic Communications Privacy Act and Computer Fraud and Abuse Act in connection with the collection of information regarding the underlying plaintiffs’ online activity for eventual dissemination to third-party advertisers, one court construed a policy that had Coverage B wording different from the wording found in the ISO form. That policy defined “personal injury offense” to include “Making known to any person or organization written or spoken material that violates a person’s right to privacy.” This took the place of the phrase “oral or written publication, in any manner” found in the ISO form.²⁹⁴ Under that non-ISO definition, the court

²⁹² *Whole Enchilada, Inc. v. Travelers*, 581 F. Supp. 2d 677, 698 (W. Dist. Pa. 2008); see also *Creative Hospitality Ventures, Inc. v. U.S. Liability Ins. Co.*, No. 08-cv-22302 (S.D. Fla. Mar. 23, 2011) (restaurant printed more than five digits of customers’ credit card numbers on printed receipts, along with expiration dates, in alleged violation of FACTA; court found no “publication” for purposes of Coverage B had occurred because the underlying complaint lacked allegations of any “dissemination of information to the public,” or even any “allegation that any FACTA-violation receipt was provided to anyone other than the cardholder.”), *aff’d*, No. 11-11781, 2011 WL 4509919, at *5 (9th Cir. Sept. 30, 2011) (“In sum, providing a customer a contemporaneous record of a retail transaction involves no dissemination of information to the general public and does not constitute publication within the meaning of Essex’s Policy.”).

²⁹³ *Bowyer v. Hi-Lad Inc.*, 609 S.E.2d 895, 912 (W.Va. 2004) (insured argued that the term “publication” was ambiguous and should be construed against the insurer to cover an employee’s underlying claim that the insured “used the surveillance system to capture his oral communications, and then publish that audio material through speakers to the officers and employees” of the insured’s business; the court held that there was “nothing in the policy indicating that the word publication necessarily means transmitting the intercepted communications to a third party, as is required of material in the defamation context. And, even were we to assume publication does require communicating to a third-party, the surveillance monitoring system apparently functioned in such a way that anyone in the manager’s office or in [the hotel owner’s] home had the ability to listen in on employee conversations”).

²⁹⁴ Some courts have distinguished between the terms “publication” and “making known” for purposes of Coverage B coverage. Compare *Motorists Mut. Ins. Co. v. Dandy-Jim, Inc.*, 182 Ohio App.3d 311, 319, 912 N.E.2d 659, 655 (Ohio App. Ct. 2009) (distinguishing “publication” from “making known” for Coverage B purposes), and *Zurich American Ins. Co. v.*

found the defendant's passage of information to its parent company and the defendant's employees sharing of the information among themselves to constitute "making known to any person or organization." (The holding was reversed on appeal but not on this point.)²⁹⁵

Further hurdles faced by insureds seeking coverage under a CGL policy for claims arising from a data breach are that, even if it overcomes the significant thresholds to coverage contained in the Coverage B insuring provisions, there are typically a number of policy exclusions applicable to Coverage B that can operate to exclude coverage. For example, the standard ISO form contains an exclusion for "personal injury and advertising injury" arising out of violation of any "statute, ordinance or regulation . . . that prohibits or limits the sending, transmitting, communicating or distribution of material or information."²⁹⁶ Other Coverage B exclusions that can potentially come into play in the event of a data breach include ones for "personal and advertising injury" arising out of the criminal act of the insured (which could come into play when employee theft is in issue); arising out of intellectual property rights; committed by insureds in media and Internet type businesses; arising out of an electronic chat room or bulletin board the insured hosts, owns or controls; arising out of breach of contract; and other exclusions that may be more general in nature but apply to the specific claim in issue, or that may be specifically manuscripted for the insured in issue.

(3) Coverage A and B Hurdle

Yet another hurdle for attempts to obtain coverage of a third-party data breach claim under a CGL Policy is the requirement under both Coverage A and Coverage B that the claim be for "sums that the insured is legally obligated to pay as damages." As discussed above, often consumers have not sustained out-of-pocket losses, or the payments in issue are the type of fines, penalties or other types of costs that do not fall within the scope of covered damages.

Fieldstone Mortg. Co., No. CCB-06-2055, 2007 WL 3268460, *5 (D. Md. Oct. 26, 2007) (same), with *State Farm General Ins. Co. v. JT's Frames, Inc.*, 181 Cal.App.4th 429, 104 Cal.Rptr.3d 573 (Cal. Ct. App. 2010) (equating the term "publication" to "making known to any person or organization" for Coverage B purposes).

²⁹⁵ *Netscape Communications Corp. v. Federal Ins. Co.*, 2007 WL 2972924 (N.D.Cal.), *reversed*, *Netscape Communications Corp. v. Federal Ins. Co.*, 2009 WL 2634945 (9th Cir., August 27, 2009). The Ninth found the policy's language regarding "any person or organization" to be dispositive. However, the Ninth Circuit disagreed with the lower court regarding the applicability of an exclusion to Coverage B. The policy excluded coverage for personal injury offenses relating to defined "online activities," including the provision of Internet access. While the lower court found that the exclusion barred coverage because the claims involved the use of software to assist with downloading files, the Ninth Circuit, reading the exclusion narrowly, reasoned that the software itself does not provide Internet access, and thus the exclusion did not apply.

²⁹⁶ For example, in *Creative Hospitality Ventures, Inc. v. U.S. Liability Ins. Co.*, 655 F.Supp.2d 1316 (S.D. Fla. 2009) (Rosenbaum, U.S.M.J.), *adopted in part, ruling reserved in part*, 655 F.Supp.2d 1316 (S.D. Fla. 2009), certain underlying claims alleging FACTA credit card violations against a restaurant were excluded from personal and advertising injury coverage under the policy's "Distribution Of Material In Violation of Statutes" exclusion (that exclusion excluded coverage for personal and advertising injury "arising directly or indirectly out of any action or omission that violates or is alleged to violate . . . [a]ny statute, ordinance or regulation . . . that prohibits or limits the sending, transmitting, communicating or distribution of material or information"). It was held that because FACTA is a "statute that limits the information that . . . an electronically printed receipt . . . may include . . . FACTA qualifies as a statute that 'prohibits and limits the . . . communicating or distribution of material or information,' within the ordinary meaning of the terms of this exclusion."

While CGL coverage issues and disputes have recently become a battleground,²⁹⁷ the field is not likely to be a static one. As policyholders attempt to find loopholes in CGL policies to trigger at least a duty to defend data breach claims in situations not contemplated by insurers or intended to be covered by such policies, any success by policyholders will likely result in insurers responding by drafting and including in policies additional exclusions and limitations on coverage directed preventing any unintended coverage from being found.

(v) Professional Liability/E&O

Most professionals and entities engaged in providing services to others have errors and omissions (E&O) liability policies in place that they look to for a defense and indemnity when a claim is asserted against them by their clients. When a data breach at least arguably occurs within the scope of covered services, particularly when it involves data of its client, such an insured may look to its professional liability/E&O insurer to at least provide a defense to any third-party claims arising from the data breach. Thus, for example, a law firm or engineering firm or technology services firm that improperly disposes of or loses client files or is involved in issues relating to planning, designing or implementing a client's software program that is involved in a breach, and is subject to client claims, may try to seek coverage under its professional liability/E&O policies.

Professional liability and other E&O policies, however, may contain electronic data or software design exclusions, although some may have exceptions for such services that are incidental to the "professional services" covered and thus trigger a duty to defend some data breach claims that arguably fall within the exception.

On the other hand, some E&O policies are designed to provide coverage for such claims. For example, many E&O policies issued to technology companies recognize that such insureds are engaged in activities likely to make them more prone than companies in other industries to involvement in electronic data breaches, either as direct targets or as vendors to others. Thus, policies available to such technology companies may also include coverages directly encompassing data breach claims.

Often the coverage issues include whether the claim is within the scope of covered services, whether the insured's error that caused the alleged damage or financial injury in question falls under policy's definition of "wrongful act," whether there are alleged to be "damages" covered

²⁹⁷ Currently pending are several lawsuits concerning requests by policy holders for coverage, or at least a defense, under Coverage B for claims arising from breach related events, such as the class actions commenced against retailers for alleged collection and use of customer ZIP Codes in violation of California's Beverly-Song Act, as well as coverage lawsuits involving Sony entities and insurers.

by the policy, and whether there is an exclusion directed at data breach or other electronic claims.²⁹⁸

(vi) D&O

As large publicized data breaches involving publicly traded companies often result in drops in company stock prices, companies and their directors and officers who are faced with such a data breach may well also face the securities/D&O claims that frequently accompany a significant and unexpected fall in stock prices and allegations of failure to disclose a significant risk. For example, following the Heartland data breach, the company's stock price fell, and shareholders pursued securities fraud litigation against Heartland on the basis that it had misrepresented the state of its computer security. While the suit was ultimately dismissed, it shows the potential for shareholder litigation against companies that are victims of data breaches.²⁹⁹

Further, with the increasing issuance by state and federal agencies of data security regulations requiring the institution of data security protocols by companies, some of which expressly require board review of data protection plans and procedures, there is likely to be a concomitant increase in D&O claims. For example, in addition to the accountability placed on boards by the Sarbanes-Oxley Act of 2002, the new federal Red Flags Rule discussed above specifically requires that the board of directors, a board committee, or a designated employee at the level of senior management be involved in the oversight, development and administration of the required identity theft prevention program. In addition, as discussed above, in October 2011, the SEC Division of Corporation Finance released a Disclosure Guidance stating that public companies

²⁹⁸ For example, the "wrongful act" coverage requirement has been found to include (at least under Minnesota law) "intentional, non-negligent acts but to exclude *intentionally wrongful* conduct." See *Eyeblaster, Inc. v. Federal Ins. Co.*, 613 F.3d 797, 804 (8th Cir. 2010) (emphasis added). In *Eyeblaster, Inc.*, a computer user sued Eyeblaster, Inc., alleging that Eyeblaster injured his computer, software, and data after he visited an Eyeblaster website. The E&O policy at issue obligated Eyeblaster's insurer "to pay loss for financial injury caused by a *wrongful act* that results in the failure of Eyeblaster's product to perform its intended function or to serve its intended purposes." The insurer conceded that the underlying claim sufficiently alleged "financial injury." Nonetheless, the insurer argued (and the district court agreed) that coverage was non-existent because Eyeblaster had acted intentionally, and thus no "wrongful act" within the meaning of the policy had occurred ("wrongful act" was defined under the policy as "an error, an unintentional omission, or a negligent act."). On appeal, the Court of Appeals for the Eighth Circuit reversed, finding that although Eyeblaster had acted intentionally in placing its software in the underlying complainant's computer, there was "no evidence that the allegations . . . spoke of intentional acts that were either negligent or wrongful." Thus, the court found that the underlying complaint had sufficiently alleged a "wrongful act" on the part of Eyeblaster within the meaning of the policy, and consequently found a duty to defend had been triggered.

²⁹⁹ *In re Heartland Payment Systems, Inc. Securities Litigation*, Civ. No. 09-1043 (D.N.J., Dec. 7, 2009). The court found that the securities fraud claims failed to meet the heightened pleading standards provided by the Private Securities Litigation Reform Act of 1995 (PSLRA). The court explained that the PSLRA requires fraud to be pleaded with particularity, and also requires plaintiffs to state with particularity facts giving rise to a strong inference that the defendant acted with the required state of mind. Citing the Supreme Court's decision in *Tellabs, Inc. v. Makor Issues & Rights Ltd.*, 551 U.S. 308 (2007), the court explained that a complaint will adequately allege state of mind only if a reasonable person would deem the inference of scienter to be at least as strong as any inference of non-fraudulent intent. The court found that the plaintiffs had failed to meet this heightened pleading requirement. In particular, the court found that the defendant's statements regarding its computer security, when examined in context, were not misleading. The court also found that the plaintiffs had failed to allege that the defendant knew or should have known that its statements were false. Having found that the complaint failed to adequately allege two of the elements of its fraud claims, the court dismissed the complaint with prejudice.

may need to disclose their exposure to cyber security risks and incidents as potential material information to be disclosed under securities law disclosure requirements and accounting standards.³⁰⁰ This also potentially provides grounds for claims against directors and officers as well as public entities alleging inadequate disclosure.

If a data breach leads to a suit by the owners of the compromised data – or by shareholders if the breach leads to a large loss to the insured company – against the allegedly responsible directors or officers, those directors and officers may look to their D&O policies to see if there is coverage (mindful, of course, of any exclusions that may apply).³⁰¹ Similarly, in the event of a securities action, the targeted company will likely look to any entity coverage provided by such policies.

(vii) Kidnap and Ransom/Cyber Extortion

Corporations and individuals operating in high-risk areas around the world often carry kidnap and ransom coverage. The policies typically provide indemnity in connection with ransom payments and personal accident losses caused by kidnapping incidents. Such policies may also cover extortion, including extortion related to a threatened introduction or activation of a computer virus to the insured's computer system unless a ransom is paid. Depending on the policy's scope of coverage, including how the policy defines "virus," such coverage may extend to a hacker's threatened use of software to capture private data.

With the increase in threats of cyber extortion in recent years, policies specifically directed at cyber extortion are now available and often offered in conjunction with specialty policy products directed at providing coverage for network security and related risks.

IV. Mitigation of Data Breach Exposures

As data breaches increase in frequency as well as severity, much of the discussion in studies and among professionals and insurers involved in data breaches has turned to scrutinizing past breaches and proposing data security procedures in an effort to reduce the likelihood of a breach and of resultant costs and damages.

³⁰⁰ . For more information regarding the recently released Disclosure Guidance, see "Public Companies May Need to Disclose their Exposure to Material Cyber Security Risks According to New Guidance Issued by SEC Division of Corporation Finance," *Edwards Wildman Palmer Client Advisory*, October 2011 (available at <http://www.edwardswildman.com/newsstand/detail.aspx?news=2634>).

³⁰¹ As to exclusions, it is possible, for instance, that the D&O policy at issue may exclude claims arising from violations of privacy rights, thus potentially limiting the scope of available coverage in the event of a data breach. See, e.g., *Resource Bank v. Progressive Cas. Ins. Co.*, 503 F.Supp.2d 789, 795-97 (E.D. Va. 2007) (insured sought coverage under its D&O policy for two class action lawsuits alleging that the insured violated the Telephone Consumer Protection Act by sending unsolicited facsimile advertisements; court held coverage was excluded, in part, on the basis of the policy's Bodily Injury and Property Damage Exclusion that excluded coverage for claims of "invasion of privacy").

1. Compliance

Many of the new state and federally statutes and regulations directed at data breach risks have as a stated goal the reduction of data breaches involving Personal Information and impose pre-breach security measures in pursuit of that goal.

Failure to comply with applicable state or federal data security statutes and regulations, or industry-established security requirements such as PCI-DSS, is a basis for fines and penalties from oversight agencies, and evidence that may be used by consumers and other claimants to demonstrate that the entity whose data was breached did not satisfy industry security standards. Compliance with applicable statutes, regulations, and industry standards is one of the strongest defenses a breached entity has against claims based on negligence. While there is increasing recognition of the costs of security breaches and the need for corporations to address information security, and increasing security requirements imposed by regulatory authorities, at least one study noted that companies view inadequate security budgets as their biggest barrier to information security, with 46% rating budget as their number one issue.³⁰² Another major study reported, however, that more of the companies studied had better-than-average security postures compared to the prior year, and that organizations with improved security postures enjoyed significantly lower data breach costs.³⁰³

2. Instituting Reasonable Security Procedures

A recent study of data breaches reported that in 96% of the cases studied, investigators concluded that the breach could have been avoided through the implementation of simple or intermediate security controls.³⁰⁴ The study also reported that the cost of a data breach is significantly less for companies that institute and exercise risk management procedures, than for those that do not.³⁰⁵ While many of the new data security regulations require companies to institute security procedures designed to reduce the risk of data breach, security plans and procedures must be consistently implemented to be effective. As discussed below, training on security procedures is critical to implementing security procedures and reducing the risk of data breach.

3. Limiting Access to Protected Information

Studies show that breaches, and the scope and cost of breaches, can be reduced by limitations on: (i) access rights, which restrict access to Personal Information and other types of confidential information only to those with a need for that access; (ii) the amount of information collected

³⁰² Deloitte, *2010 TMT Global Security Study – Key findings*.

³⁰³ Ponemon Institute, LLC, *2010 Annual Study: U.S. Cost of a Data Breach*.

³⁰⁴ *2011 Data Breach Investigations Report*, A study conducted by the Verizon RISK Team in cooperation with the United States Secret Service and the Dutch High Tech Crime Unit.

³⁰⁵ Verizon RISK Team, *2011 Data Breach Investigations Report, supra*.

and stored; and (iii) the duration of time Personal Information is retained, to only that which is necessary. These limitations are the focus of both data security regulations and risk management protocols.

4. Training/Awareness

Human error of some kind (by employees, customers, suppliers or other third parties) has been reported to be involved in a large number of breaches. One study reported that 41% of breaches in 2010 were attributed to negligence.³⁰⁶

Data breaches often occur when companies and their employees fail to consider the risk of data breaches from routine conduct, or to comply with applicable data security requirements.

Resultant claims arise from lack of awareness by companies and their employees of applicable governmental data security requirements, and their own non-compliance.

Relatively simple measures that can reduce the risk of data breach include:

- Educating company executives as to applicable legal requirements governing data security and the importance of establishing a team of appropriate internal personnel and external resources to: (i) identify the type and location of protected Personal Information collected, used, stored and transmitted by the company; (ii) access the risks related to such information; and (iii) draft and propose appropriate and compliant procedures for security;
- Ensuring that paper records with Personal Information and other confidential information are shredded before disposal, and properly disposed of;
- Immediately terminating an employee's access to computer terminals and company databases on-site and off-site as soon as the employee's employment is terminated or the employee resigns;
- Instituting password requirements for access to databases with Personal Information and other confidential information, and avoiding sharing them;
- Instituting password requirements for laptops and PDAs, which are susceptible to being lost or stolen, and reminding employees not to paste the password on the laptop or PDA;

³⁰⁶ Ponemon Institute, LLC, *2010 Annual Study: U.S. Cost of a Data Breach*.

EDWARDS WILDMAN PALMER LLP

- Considering encrypting electronic documents with sensitive information before transmitting; and
- Confirming service partners such as vendors to which documents with Personal Information and other confidential information are provided have appropriate and compliant data security procedures in place, and amending contracts to require such compliance.

Often training and reminders of simple precautions can dramatically reduce the risk of data breach, at low cost to companies.

Conclusion

Data breaches, and resultant direct and indirect costs, are a growing exposure in our society. Concomitant with that exposure is the increase in state and federal laws and regulations in the U.S., and the increase in regulation in other countries, imposing data security procedures on a wide range of entities. Companies in all lines of business are subject to these exposures, and to the increasing regulatory and other legal requirements to institute data security procedures in advance of a data breach, and respond in a timely and appropriately manner once a breach occurs.

In addition, new technologies, social media practices, and online behavior tracking practices are raising new privacy issues, with increasing regulatory scrutiny, legislation, and litigation.

Contact Information:

Mark E. Schreiber
Chair, Privacy and Data Protection Group
Edwards Wildman Palmer LLP
111 Huntington Avenue
Boston, MA 02199
617-239-0585
mschreiber@edwardswildman.com

Laurie A. Kamaiko
Co-chair, Privacy and Data Protection Group
Edwards Wildman Palmer LLP
750 Lexington Avenue
New York, NY 10022
212-912-2768
lkamaiko@edwardswildman.com

EDWARDS WILDMAN PALMER LLP

Theodore P. Augustinos
Co-chair, Privacy and Data Protection Group
Edwards Wildman Palmer LLP
20 Church Street
Hartford, CT 06103
860-541-7710
taugustinos@edwardswildman.com

Edwards Wildman Palmer LLP's Privacy & Data Protection Group is an inter-disciplinary multi-jurisdictional team of attorneys with considerable experience in addressing matters related to data breaches and the obligations imposed by data protection laws in the U.S., U.K., and other countries, as well as other cyber risk exposures.

The Chairs of the Group acknowledge with appreciation the invaluable assistance provided by Edwards Wildman Palmer LLP Partners, Counsel and Associates in the preparation of this edition of our White Paper. Our thanks to Michael Bennett, Karen Booth, Eric Fader, Theo Godfrey, Richard Graham, Brian Green, Gregory Hoffnagle, Dominique Shelton, David Sigmon, Socheth Sor and Vincent Vitkowsky.