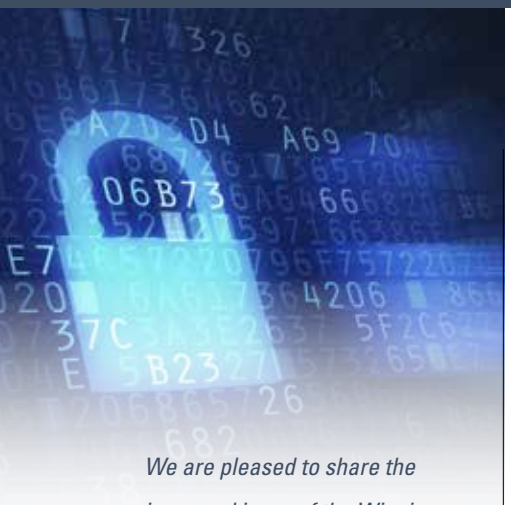
CYBERSECURITY UPDATES

FEBRUARY 2014



*We are pleased to share the inaugural issue of the Wiggin and Dana **Cybersecurity and Privacy Practice Group** Newsletter. We will circulate this newsletter periodically by e-mail to bring to the attention of our colleagues the latest updates in the areas of cybersecurity and privacy, with reports on recent developments, cases and legislative/regulatory actions of interest, as well as happenings at Wiggin and Dana. We welcome your comments and questions.*

Group Chairs:

MICHELLE DEBARGE

DAVID HALL

JOHN KENNEDY

IN THIS ISSUE

Save the Date: 2014 Connecticut Privacy Forum
Senator Richard Blumenthal to Headline

On **April 25, 2014** Wiggin and Dana will be hosting the 2014 Connecticut Privacy Forum from 8:00 a.m. - 2:00 p.m. at the Omni New Haven Hotel at Yale. This half-day conference will focus on a range of cybersecurity and data privacy compliance issues relevant to businesses in all economic sectors. Panels and presentations will address the current state of cybersecurity risk for U.S. businesses, the emerging legal and regulatory requirements, practical approaches to meaningful cybersecurity preparedness and risk management, and risk transfer through cyber-liability insurance products.

Keynote speaker, **Senator Richard Blumenthal**, will address the state of U.S. privacy in the emerging cybersecurity regime. Speakers will include leading policy makers, regulators, law enforcement officials, consultants and legal counsel. We are currently working on finalizing topics and a formal invitation will follow soon.

IndustryNEWS

Federal Contractors: Meet the New Cybersecurity Standards or Lose Your Government Book

On January 23, 2014, Secretary of Defense Chuck Hagel and General Services Administration Administrator Daniel Tangherlini sent a strong message to federal contractors and their suppliers: practice cybersecurity or the government will look elsewhere for the $500 billion in goods and services it procures annually. Hagel and Tangherlini delivered this message in a report to the White House titled, "Improving Cybersecurity and Resilience through Acquisition," which contains six recommendations designed to integrate cybersecurity into the Federal Acquisition System.

Significantly, the Report recommends that for federal acquisitions with cyber-risk, the government should not do business with companies unless those companies meet baseline cybersecurity requirements "in both their own operations and in the products and services they deliver." Federal contractors and their suppliers should be prepared to defend their cybersecurity programs—or to find another customer.

FTC Privacy Enforcement and NTIA Agenda for 2014

In December 2013, the Federal Trade Commission (FTC) and the National Telecommunications & Information Administration (NTIA), a bureau within the Department of Commerce, announced privacy initiatives for 2014 that will affect a wide array of industries. The FTC will host a series of seminars to examine the privacy implications of three new areas of technology: mobile device tracking, alternative scoring products, and consumer-generated and controlled health data. The seminar on mobile device tracking will review the practice of tracking consumers' movements throughout retail stores by identifying signals emitted by their mobile devices. The alternative scoring products seminar will focus on the use of data compiled by information brokers to predict customer behavior. Finally, the consumer-generated and controlled health data seminar will examine the privacy concerns that arise with the increasing use of health apps, online health tools, and connected personal fitness devices. With these seminars, the FTC hopes to understand the extent to which consumers are tracked, whether notice and choice are provided, and how this data is secured. Additionally, the seminars will likely lay the groundwork for future enforcement actions.

The FTC will also likely continue its focus on unfair or deceptive data security practices, children's online privacy, and the emerging market for the "internet of things"—smart, internet-enabled devices in cars, homes and offices. At an FTC workshop in November 2013, FTC Chairwoman Edith Ramirez explained that "the expansion of the Internet of Things presents three main challenges to consumer privacy: first, it facilitates the collection of vastly greater amounts of consumer data; second, it opens that data to uses that may be unexpected by consumers; and third, it puts the security of that data at greater risk." Chairwoman Ramirez went on to say that the FTC will be watching to see that companies undertake three critical steps in their design and marketing of internet connected hardware: building in consumer privacy protections from the outset, so-called privacy by design; using data only for the purposes for which the consumer agrees to provide it; and providing proper security features on internet connected hardware to protect consumer privacy. The FTC staff is preparing a report on internet connected devices, expected to be issued in mid-2014, which will provide a set of best practices for managing privacy and security. As the FTC moves forward on its 2014 agenda, an increased number of enforcement actions is likely against companies that fail to provide reasonable security for data collected from internet connected devices.

Also in December 2013, the NTIA launched a new privacy multi-stakeholder process on the commercial use of facial recognition technology. The NTIA noted three consumer privacy challenges related to facial recognition technology: securing sensitive biometric data, providing transparency when facial recognition systems are implemented in public places, and developing meaningful controls for consumers. The NTIA's goal is to develop a code of conduct for industry to adopt to improve the privacy and data security practices surrounding facial recognition systems. If implemented, the NTIA's code of conduct will set forth a blueprint for addressing privacy concerns with facial recognition technology. The first NTIA multi-stakeholder meeting was held on February 6, 2014; additional meetings will follow.

Both the FTC (http://www.ftc.gov/news-events/press-releases/2013/12/ftc-host-spring-seminars-emerging-consumer-privacy-issues) and NTIA (http://www.ntia.doc.gov/blog/2013/privacy-and-facial-recognition-technology) meetings will be open to the public.

FROM
TheCOURTS

HIPAA Enforcement Update

The United States Department of Health and Human Services' (HHS) Office for Civil Rights (OCR) continues to intensify HIPAA enforcement efforts, and HIPAA settlements have been stretching above the million dollar mark. Recent settlements provide an important glimpse into OCR's enforcement priorities and government standards for compliance. Following are summaries of three recently publicized HIPAA settlements:

ADULT & PEDIATRIC DERMATOLOGY, P.C.

On December 26, 2013, OCR entered into the first HIPAA settlement with a covered entity for failure to have policies and procedures in place to address breach notification. Adult & Pediatric Dermatology, P.C., of Concord, Mass., (APDerm), a 12-physician private practice that delivers dermatology services in Massachusetts and New Hampshire, agreed to pay $150,000 and implement a corrective action, which includes providing reports to OCR.

On October 7, 2011, APDerm filed a report with OCR regarding an unencrypted thumb drive containing the electronic protected health information (PHI) of approximately 2,200 individuals that was stolen from a vehicle of one of its staff members. The drive was never recovered. Despite the fact that APDerm timely reported the theft to OCR, notified its patients of the theft of the thumb drive within 30 days of its theft, and provided media notice, OCR opened an investigation into APDerm's HIPAA compliance and concluded that APDerm violated HIPAA by (1) not conducting an accurate and thorough analysis of the potential risks and vulnerabilities to the confidentiality of PHI as part of its security management process, and (2) not having written policies and procedures and training members of its workforce regarding HIPAA's breach notification requirements.

AFFINITY HEALTH PLAN, INC.

On August 15, 2013, OCR announced its settlement for $1,215,780 with Affinity Health Plan Inc. ("Affinity"), a not-for-profit managed care plan serving the New York metropolitan area. According to the government press release, in 2010, CBS Evening News purchased a photocopier previously leased by Affinity that still contained confidential medical information on the hard drive. CBS televised its finding, reporting that it was able to retrieve 300 pages of medical records from Affinity's old copier, including drug prescriptions, blood test results and a cancer diagnosis. On April 15, 2010, Affinity reported the breach to OCR and notified 409,000 of its members of the data breach, even though no evidence was found that the data was misused.

OCR alleged that Affinity impermissibly disclosed the PHI of up to 344,579 individuals when it returned multiple photocopiers to its leasing agent without erasing the data contained on the copier hard drives. HHS focused on the fact that Affinity allegedly failed to incorporate the electronic PHI stored in the copier's hard drives in its Security Rule risk analysis and to implement corresponding policies and procedures. As part of the settlement, Affinity also agreed to enter a corrective action plan, requiring it to use its "best efforts" to retrieve and safeguard all hard drives that were contained in photocopiers that it previously leased. Also, Affinity agreed to conduct a comprehensive risk analysis of the security risks and vulnerabilities of all electronic equipment and systems controlled, owned or leased by Affinity, and to develop a plan to address and mitigate any identified security risks and vulnerabilities.

WELLPOINT INC.

On July 8th, 2013, WellPoint Inc. ("WellPoint"), an Indiana managed care company, agreed to pay $1.7 million to settle allegations of HIPAA noncompliance. HHS's investigation of WellPoint was triggered by WellPoint's breach notification report to OCR in 2010, disclosing that security weaknesses in an online application database left the electronic PHI of 612,402 WellPoint beneficiaries accessible to unauthorized individuals over the Internet.

Although no actual unlawful access to the PHI was specifically alleged, OCR concluded that WellPoint violated HIPAA not only by impermissibly disclosing the PHI of hundreds of thousands of individuals, but also by failing to implement policies and procedures for authorizing access to the PHI maintained in its web-based application database. WellPoint had implemented a software upgrade for the database, but allegedly did not perform an adequate technical evaluation of the new software or implement appropriate technology to safeguard the PHI. In publicizing this settlement, OCR highlighted the additional

FROM
TheCOURTS CONTINUED

security risks in "applications or portals that are used to provide access to consumers' health data using the Internet" and warned covered entities and business associates to "always consider the risks to PHI when implementing changes to their information systems."

Aaron's Rent-To-Own Chain Settles FTC Charges That It Enabled Computer Spying by Franchisees

On October 22, 2013, Aaron's, Inc., a national, Atlanta-based rent-to-own franchise, settled Federal Trade Commission charges that it knowingly played a direct and vital role in its franchisees' installation and use of software on rental computers that secretly monitored consumers, including taking webcam pictures of them in their homes. Aaron's franchisees allegedly used the software to secretly track consumers' locations, capture images through the computers' webcams, and activate keyloggers that captured users' login credentials for email accounts and financial and social media sites. The FTC's complaint alleged that Aaron's knew about the privacy-invasive features of the software, but nonetheless allowed its franchisees to access the software, known as PC Rental Agent, and actually instructed them regarding how to install and use the software. In addition, Aaron's stored data collected by the software for its franchisees and also transmitted messages from the software to its franchisees. It should be noted that the same software was the subject of other 2013 FTC actions against the software manufacturer and several rent-to-own stores that used it, including Aaron's franchisees.

Pursuant to the terms of the proposed consent agreement with the FTC, Aaron's is banned from using monitoring technology that captures keystrokes or screenshots, or activates the camera or microphone on a consumer's computer, except to provide technical support requested by the consumer. Aaron's must give clear notice and get express consent from consumers at the time of rental in order to install technology that allows location tracking of a rented product. The settlement also prohibits the company from deceptively gathering consumer information. Furthermore, Aaron's may not use any information it obtained through improper means in connection with the collection of any debt, money or property as part of a rent-to-own transaction. The company must delete or destroy any information it has improperly collected and must transmit in an encrypted format any location or tracking data it collects properly. Aaron's also is required to conduct annual monitoring and oversight of its franchisees and hold them to the requirements in the agreement that apply to Aaron's and its corporate stores, and to terminate the franchise agreements of franchisees that do not meet those requirements.

FROM
TheREGULATORS

Department of Defense Issues Final Rule Amending Defense Federal Acquisition Regulation Supplement to Safeguard Unclassified Controlled Technical Information

On November 18, 2013, the Department of Defense (DoD) issued a final rule amending the Defense Federal Acquisition Regulation Supplement (DFARS), which imposes heightened security safeguards and mandatory reporting requirements for DoD contractors handling unclassified controlled technical information stored on information technology systems and databases. "Unclassified controlled technical information" is defined as information with a "military or space application" that is technical data, computer software, and any other technical information covered by DoD Directive 5230.24, "Distribution Statements on Technical Documents," or DoD Directive 5230.25, "Withholding of Unclassified Technical Data from Public Disclosure." It refers to information that is "sensitive but unclassified," and thus has certain restrictions on how it must be stored, accessed, transmitted and shared.

The rule establishes modified DFARS contract provisions that must be included in all contracts between DoD and DoD contractors that have access to controlled technical information stored on the DoD contractors' computer systems and databases. The contract provisions require the DoD contractor to implement certain information security procedures promulgated by the National Institute of Standards and Technology (NIST), which cover fourteen areas of information security, including access control, accountability,

FROM
TheREGULATORS CONTINUED

incident response, and risk assessment. The contract provisions also mandate self-reporting to the DoD within seventy-two hours of a "cyber incident" affecting covered controlled technical information, and require maintenance of certain evidence for ninety days if a contractor's or subcontractor's network is subject to a cyber incident. Finally, the contract provisions include a flow-down clause that requires all downstream contractors to comply with the same cybersecurity obligations.

DFARS parallels two related efforts within the DoD and other government agencies: the October 2013 memorandum issued by Secretary of Defense Hagel, which seeks to develop heightened standards for the safeguarding of sensitive but unclassified information, and Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," which directed NIST to develop and issue a Cybersecurity Framework.

NIST Framework Version 1.0 Released

On February 12, 2014, the National Institute of Standards and Technology (NIST) released Version 1.0 of the Framework for Improving Critical Infrastructure Cybersecurity (the Framework). The release is the culmination of months of public discussion on earlier drafts released last year. Recognizing that the national and economic security of the United States depends on the reliable functioning of critical infrastructure, Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," directed the NIST to work with stakeholders to develop a voluntary framework for reducing cyber-risks to critical infrastructure. The Framework consists of a cybersecurity risk management model based on five high-level security functions (Identify, Protect, Detect, Respond, Recover), coupled with more detailed subcategories and references to existing recognized standards, guidelines, and best practices to promote cybersecurity in the nation's critical infrastructure. The Framework also includes a methodology for companies to establish a cybersecurity "profile" to align risk management measures with business requirements and set goals, as well as several "tiers" which businesses can use to evaluate the degree to which they have integrated the Framework into their business. The prioritized, flexible, repeatable, and cost-effective approach of the Framework is designed to help owners and operators of critical infrastructure to manage cybersecurity-related risk while protecting business confidentiality, individual privacy and civil liberties.

Version 1.0 of the Framework does not dramatically differ from the original release, although industry groups succeeded in having the original privacy and civil liberties appendix to the Framework removed on the grounds that the appendix inappropriately imposed "fair information practices" (FIPs) too broadly across the private sector. Many objected that regulated businesses are already subject to distinct privacy frameworks, that some aspects of the Framework do not touch upon privacy interests, and that the FIPs may not be an appropriate benchmark for protecting privacy in the context of cybersecurity. Instead of the original privacy appendix, Version 1.0 incorporates a modified approach that will allow organizations to better incorporate general privacy principles when implementing a cybersecurity program. This methodology was developed through discussions with representatives of a variety of industry sectors and in the revised version still reflects the use of FIPs.

Still open is the issue of what "adoption" of the Framework means, how it would be gauged, and whether or not specific steps needed to be taken in order for an organization to be considered as having adopted the Framework. In public hearings prior to the release of Version 1.0, there was general consensus that the organizations were "adopting" the Framework if they were using it as a part of their risk management process, consistent with the following definition: "An organization adopts the framework when it uses the Cybersecurity Framework as a key part of its systematic process for identifying, assessing, prioritizing, and/or communicating: cybersecurity risks, current approaches and efforts to address those risks, and steps needed to reduce cybersecurity risks as part of its management of the organization's broader risks and priorities."

It remains to be seen whether private sector participants in the Framework discussions will now take the ball and help advance the Framework's use in the critical infrastructure. Many issues remain open, not the least of which is whether legislation in this area will issue, and whether such legisation will include incentives for private sector businesses to share incident information with the government. Other issues to be addressed include the health, safety, and environmental aspects of cybersecurity considerations specific to industrial control systems and compatibility of the Framework with international standards.

FirmNEWS

Wiggin and Dana Cybersecurity and Privacy Practice Group

Wiggin and Dana is pleased to announce the formation of its Cybersecurity and Privacy Practice Group, a multi-disciplinary team drawing on attorneys from a range of firm practice groups. Recognizing that the emerging cybersecurity framework calls for comprehensive and integrated approaches to security across the entire enterprise, the Practice Group pulls together the diverse strengths of the firm's technology, compliance, investigation, insurance, healthcare and litigation practices.

The Practice works with clients in meeting the challenges of protecting enterprise security and maintaining compliance with privacy laws during a time of rapid technological and legal change, increasingly sophisticated external and internal threats to corporate and government information systems.

Wiggin and Dana offers comprehensive cybersecurity and privacy services to clients, including:

- Development of comprehensive compliance programs for information security, data privacy policies and data governance
- Assistance with data breach preparedness and data breach response programs and related post-breach investigations
- Representation in connection with government investigations of data incidents, including investigations by state attorneys general and the Federal Trade Commission
- Defense of claims, including class actions, arising from data breaches
- Transactional advice on privacy and security matters in outsourcing, cloud computing, mobile services, technology contracts, mergers and acquisitions, and cross-border data transfer
- Counseling on health care data and systems security and privacy, including compliance assessments under HIPAA, HITECH and state health care laws
- Advice to insurance carriers and insureds in connection with cyber-risk coverage matters
- Advice on e-discovery and records retention programs
- Counseling of institutions of higher education on privacy issues under FERPA and state law and non-profit institutions on data privacy and security compliance
- Preparation of security and privacy awareness training programs for clients

WIGGIN AND DANA PARTNERS AND COUNSEL CYBERSECURITY AND PRIVACY

Export Compliance: Jim Glasser, David Hall, Tahlia Townsend

Health Care: Michelle DeBarge

Insurance: Jim Glasser, Tim Diemand, Michael Menapace

Labor and Employment: Mary Gambardella, Lawrence Peikes

Litigation (General) and Consumer Protection: Aaron Bayer, Bob Langer, Kim Rinehart, Kevin Smith

Litigation (White Collar, Corporate Compliance): Margery Feinzig, Jim Glasser, Dave Hall, Joe Martini, Rob Hoff

Privacy and Information Security: Aaron Bayer, Michelle DeBarge, Bob Langer, Mark Heaphy, John Kennedy

Technology and Outsourcing: Mark Heaphy, Niket Rele, Sarvesh Mahajan, Tamia Simonis, John Kennedy

Wiggin and Dana Cybersecurity and Privacy Practice Group

For more information, please see the full Cybersecurity and Privacy Practice Group description at www.wiggin.com/12280, or contact:

MICHELLE DEBARGE
860.297.3702
mdebarge@wiggin.com

DAVID HALL
215.988.8325
dhall@wiggin.com

JOHN KENNEDY
203.363.7640
jkennedy@wiggin.com

About Wiggin and Dana LLP

Wiggin and Dana is a full service firm with more than 150 attorneys serving clients domestically and abroad from offices in Connecticut, New York and Philadelphia. For more information on the firm, visit our website at www.wiggin.com.