Attorney Advertising

Robinson+Cole

Data Privacy and Security Insider

May 21, 2015

DATA BREACH

CareFirst Announces Breach of 1.1 Million Records in Cyberattack

Following in the footsteps of Anthem and Premera, CareFirst, a Blue Cross Blue Shield plan servicing customers in Maryland, Washington, D.C. and Virginia announced yesterday that it too has been the victim of a "sophisticated" cyberattack that exposed customer information to hackers. After the announcements by Anthem and Premera, the CEO of CareFirst hired a well-known security firm to review its systems. The security firm confirmed that a successful intrusion occurred in June of 2014. The intrusion allowed hackers to obtain access to customer names, dates of birth and email addresses, but NOT financial information, including Social Security numbers.

The hacking is being investigated by the FBI, along with the Anthem and Premera incidents. Sources have indicated that they all may be related, and some surmise that they were state sponsored. At any rate, good for CareFirst for proactively checking its system, especially when the health care industry has been a clear target and will continue to be a target by hackers.

– Linn Foster Freedman

Hackers Seek to Access Intellectual Property Assets of Higher Educational Institutions

College and universities, like many other businesses and organizations, defend against millions of cyberattacks each day. Most recently, Penn State's College of Engineering discovered a multi-year long cyberattack seeking usernames and passwords of students, faculty, and staff. The University hired consultant Mandiant to investigate the breach. Mandiant discovered two separate attackers and determined that at least one was from China.

Hackers often target colleges and universities because they are rich sources of information. First, large universities have personal information files on thousands of individuals - students, faculty, and staff members. Additionally, the university likely has personal financial data for tuition payments and ticket sales. Most significantly, however, universities have valuable intellectual property and technology research files, the result of work by professors, graduate students and their sponsoring company collaborators. Much of the research is not yet protected by patent filings and so is very vulnerable to theft.

Because of Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99), a federal law that protects the privacy of student's personal information, higher educational institutions have policies and practices in place to educate and safeguard against the transfer of student data. However, these efforts have not generally focused on defending against a cyberattack. Additionally, the organizations also have a large number of users with password protected access to some or all of their IT systems, and thus hackers have many opportunities to exploit vulnerabilities in the system to gain access.

– Kathleen M. Porter

INSURANCE COVERAGE

Data Breach Coverage Denial Upheld by Connecticut Supreme Court

In a 3 page per curiam decision issued this week, the Connecticut Supreme Court upheld a lower court's decision holding in *Recall Total Information Management, Inc., et. al v. Federal Insurance Company*, that Federal Insurance Co. and Scottsdale Insurance Co. commercial general liability policies did not provide coverage for losses of IBM contractors relating to a data breach from the loss of computer tapes. The incident occurred in 2007, when a cart holding computer tapes fell out of the back of a transportation company's van on a highway exit ramp. Although the tapes could not be read on a personal computer and there was no indication that the information on the tapes was accessed, the tapes contained Social Security numbers, dates of birth and contact information of 500,000 IBM employees. It was reported that 130 of the tapes were removed by the roadside and were not recovered. The IBM employees were notified of the incident, but there was no evidence to indicate that any IBM employee was injured as a result of the incident.

The contractors sought insurance coverage for losses sustained from the incident and argued that the losses constituted personal injuries caused by the publication of material that violates a "person's right to privacy." They argued that the publication occurred when the IBM employees' data was published "to a thief." The appeals court disagreed, stating that "…we believe that access is a necessary prerequisite to the communication or disclosure of personal information, ...the plaintiffs have failed to provide a factual basis that the information on the tapes was ever accessed by anyone." The appeals court also held that a state law requiring notification of a data breach does not create a personal injury that would trigger coverage under the policies.

The Connecticut Supreme Court stated: "We…adopt the Appellate Court's opinion as the proper statement of the issue and the applicable law concerning that issue."

Insurance coverage cases of first impression, including for data breaches, are winding their way through the court system and will have important precedential effect. We are watching them closely and will keep you apprised of their development.

– Linn Foster Freedman

ENFORCEMENT AND LITIGATION

FTC Sued by Blogger to Release Data Security Guidelines

The Federal Trade Commission (FTC) was sued this week by Philip Reitinger, a fellow blogger and former Deputy Undersecretary of the Department of Homeland Security. He is now President of VisionSpear LLC, an information security and privacy company.

In November of 2014, Mr. Reitinger sent a FOIA request to the FTC requesting FTC "records describing standards, guidelines, or criteria for what conduct or omission constitutes an unfair act or practice in or affecting commerce authorizing FTC action, and criteria for bringing such an action, under 15 U.S.C. § 45, related to data or cyber security."

Reitinger alleges in the suit that The FTC "failed to disclose a single record in response to this request." The FTC alleged that it was unable to provide the documents as they were "deliberative and pre-decisional" or "attorney work-product." Reitinger is asking the Court to order the FTC to immediately disclose all responsive records, and for declaratory and injunctive relief against the FTC.

The FTC has been on the hot seat in this area for some time, and has been challenged by both Wyndham Worldwide and LabMD for exceeding its authority in enforcing data security practices of companies that have suffered data breaches. This is another challenge to the FTC's authority that we will be watching closely.

– Linn Foster Freedman

At Least 90 Class Actions Primed for Consolidation Relative to 2015 Anthem Data Breach

On February 4, 2015, health insurer Anthem disclosed a data breach affecting the personal and financial information of up to eighty million Anthem members throughout the United States. Beginning the very next day, class action lawsuits began to be filed alleging a variety of missteps by Anthem, including a failure to encrypt personal information, delays in disclosing the breach and failing to adequately protect member data despite paying $1.7 million in fines in 2011 and 2012 to redress earlier alleged failures to safeguard information.

To date, more than ninety class actions have been filed throughout the country. One plaintiff filed a motion to consolidate these lawsuits before the Federal Judicial Panel on Multi-District Litigation for the Southern District of Indiana – In re: *Anthem, Inc. Customer Data Security Breach Litigation*, MDL Docket No. 2617.

While it appears consolidation is inevitable, there is some dispute amongst the various plaintiffs and Anthem as to the proper forum for the proposed multi-district litigation. The two leading candidates are the Southern District of Indiana (where Anthem is headquartered) and the Central District of California (the state where the largest number of individuals affected by the data breach reside).
A hearing date has not yet been scheduled on the motion to consolidate. The substantive merits of the litigation will likely not move forward until the consolidation issue is addressed.

We will keep you advised of updates as they arise.

– Brian J. Wheelin

Another Multi-Million Dollar TCPA Settlement

TCPA settlements are becoming ho-hum because they are so frequent. They are plaintiffs' attorneys' dream cases because of strict liability damages. All the more reason to keep your eye on the TCPA compliance ball as it continues to be a compliance officer's worst nightmare.

Doctor Diabetic Supply LLC, a medical supply company, consented to a $2.2 million judgment for sending 4,324 unsolicited junk faxes to medical practices in Cincinnati. Watch those faxes, text messages and robocalls—they could cost you significant money if you don't comply.

–Linn Foster Freedman

Employer Sued for Invasion of Privacy by Tracking its Employees' Every Move – On and Off Company Time

Can your employer track you 24-7? This plaintiff, Myrna Arias, a former-Intermex sales executive, claims that her employer's constant tracking of her every move violated her privacy rights. In Bakersfield, California, Arias' employer required her and her fellow employees to download a mobile app that tracked geolocation, called Xora, that ran constantly on their iPhone. Arias refused to allow her employer track her movements during non-work hours and uninstalled the mobile app, which was against her employer's policy. Intermex's response was to fire her. Arias filed a suit against Intermex for invasion of privacy, retaliation, unfair business practices, and damages over $500,000.

In Arias' complaint, she said:

Xora contained a global positioning system (GPS) function which tracked the exact location of the person possessing the smart phones on which it was installed. After researching the app and speaking with a trainer from Xora, [Arias] and her co-workers asked whether Intermex would be monitoring their movements while off duty. [Intermex] admitted that employees would be monitored while off duty and bragged that he knew how fast she was driving at specific moments ever since she had installed the app on her phone. [Arias] expressed that she had no problem with the app's GPS function during work hours,

but she objected to the monitoring of her location during non-work hours [. . .] ***She likened the app to a prisoner's ankle bracelet****.*

Intermex allegedly not only told her co-workers about her driving speed, but also about the specific routes she took, and the amount of time she spent at each customer location. Intermex's monitoring of not only Arias' company time, but of her personal time as well seems to cross the line. We will monitor this case to see the outcome and what type of precedent is set for other employers who want to use geolocational data to ensure employee efficiency.

– Kathryn M. Sylvia

RadioShack Bankruptcy Court Approves Sale of Personal Information Collected by Debtor

Earlier this year, an affiliate of the hedge fund Standard General LP assumed more than 1,700 RadioShack® store leases in an auction sale in the electronics retailer's bankruptcy. Standard General reportedly plans to partner with Sprint® to open stores within more than 1,400 of these RadioShack locations. Sprint branded mobile devices, including Boost® and Virgin Mobile®, will be sold by Sprint employees in the Sprint stores within the RadioShack stores. The storefronts and promotional materials will bear the Sprint brand, but the locations will also carry some other historical RadioShack products, services and accessories.

In addition to its store leases, RadioShack's assets included its name and other IP assets, as well as a substantial amount of personal information collected from millions of consumers prior to the bankruptcy. This personal information includes names, addresses, telephone numbers, email addresses, and records of purchased items. In a second bankruptcy court auction, which was approved by the bankruptcy court on May 29, Standard General paid $26.2 million for these assets.

Yesterday, the bankruptcy court approved the sale over the objections of several parties, including the Federal Trade Commission (FTC) and third party manufacturers Apple and AT&T who sold products to the bankrupt retailers. The approval also came after RadioShack successfully negotiated a settlement with several state attorneys general to limit the buyer Standard General's access to (i) RadioShack customer email to the last two years, and (ii) other RadioShack customer information to only 7 of 170 fields of data collected by RadioShack.

The FTC's objection was made to the court-appointed consumer privacy ombudsman in the RadioShack bankruptcy. Specifically, the FTC's letter alleged the sale of personal information constitutes a deceptive practice because in its privacy policy, RadioShack promised never to share the customer's personal information with third parties. In its letter to the RadioShack ombudsman, the FTC requested that the Toysmart case precedent be followed to (i) prohibit the sale of personal customer information as a standalone asset; (ii) restrict any sale of such information only to a third party who is in the same business as RadioShack, and who agrees to be bound by and follow the terms of RadioShack's privacy policies as to the acquired information and (iii) to obtain affirmative consent from consumers for any material changes to the applicable privacy policy. Alternatively, the FTC stated that the debtor could seek its customers' affirmative consent to the transfer of data, and the information could be purged if customers did not grant consent.

In addition to the objections by the FTC and state attorneys, the RadioShack bankruptcy court heard but rejected separate objections by wireless carrier AT&T and device maker Apple. The companies claimed that they, and not RadioShack, owned and therefore controlled the personal consumer information collected from sales of their respective products at RadioShack. In the case of AT&T, if a consumer purchased an AT&T product at RadioShack, AT&T claimed ownership of that consumer's personal information (not simply the transaction information) and wanted it withheld from the sale to Standard General. Similarly, in Apple's motion, Apple claimed its reseller agreement with RadioShack provided that it owned all information it collected from its end users, including their identity. As such, Apple claimed ownership of the personal information related to any purchase of an Apple product at RadioShack and requested it be withheld from any sale. AT&T and Apple both expressed concern about protecting consumers' privacy in their motions. Neither address whether RadioShack's privacy policy adequately disclosed to RadioShack consumers that their personal information collected as part of the purchase of certain products at RadioShack would be owned and controlled by third party manufacturers, such as AT&T or Apple. Additionally, the fact that Sprint, a competitor of Apple and AT&T, is partnering with the potential acquirer of the personal information was likely a factor in Apple and AT&T challenging the transfer.

RadioShack claimed segregating this customer information was not done initially and therefore would be difficult if not impossible to do now. The RadioShack court ultimately approved the sale, and ruled against the FTC, AT&T, Apple and RadioShack customers.

See In re RadioShack Case No. 15-10197 (BLS).

– Kathleen M. Porter

SOCIAL MEDIA

Connecticut Becomes Newest State with Social Media Privacy Law

Connecticut Governor Daniel Malloy signed Connecticut's new social media law on Tuesday, May 19, 2015 prohibiting employers from:

1. requesting or requiring that an employee or applicant provide the employer with a user name and/or password, or any other authentication means for accessing a personal online account;
2. requesting or requiring that an employee or applicant authenticate or access a personal online account in the presence of the employer;
3. requiring that an employee or applicant invite the employer or accept an invitation from the employer to join a group affiliated with any personal online account of the employee or applicant;
4. discharging, disciplining, discriminating against, retaliating against or otherwise penalizing any employee who refuses to provide the employer with the means to accessing a personal online account,
5. fails or refuses to hire any applicant as a result of his or her refusal to provide the employer with access to the online account.

The law does not prohibit an employer from requesting or requiring an employer access to an account or service provided by the employer for the employer's business purposes. In addition, the law allows an employer to fire, discipline or penalize an employee who has transferred an employer's proprietary, confidential, or financial information to or from a personal online account. Similarly, employers are allowed under the law to conduct an investigation for ensuring compliance with state and federal laws or employee misconduct based on receipt of information about an employee's online conduct or misappropriation of employer data.

Complaints that an employer has violated the law are filed with the Labor Commissioner. After hearing, the commissioner may levy a civil penalty of up to $500 for the first violation and $1,000 for each subsequent violation and award the employee appropriate relief, including rehiring, back wages, benefits or "any other remedies that the commissioner may deem appropriate." The commissioner may also request that the Attorney General bring an action in Superior Court to recover penalties levied against the employer. Employers should keep tabs on new social media laws as they are developed so policies can be adjusted and compliance monitored.

– Linn Foster Freedman

American Hospital Association Releases Social Media Guide

On May 13, 2015, the American Hospital Association (AHA) issued "A Hospital Leadership Guide to Digital & Social Media Engagement." The Guide is as hip as can be for the AHA, and provides easy to understand and practical tips for hospital leadership to delve into the rapidly changing social media landscape.

The Guide is broken into 4 basic categories:

1. Getting Started;
2. Setting up An Infrastructure;
3. Engaging Patients; and
4. Engaging Employees.

The tips are within each category. The entire Guide is user friendly and a great tool for hospital leadership.

– Linn Foster Freedman

DRONE PRIVACY

Commercial UAS Modernization Act Introduced to the Senate; We Can't Wait for the FAA

On May 12, 2015, the Commercial UAS (Unmanned Aerial Systems –i.e. drones) Modernization Act was introduced to the Senate Subcommittee on Aviation Operations, Safety and Security, which sets forth interim drone operating rules while the Federal Aviation Administration (FAA) finalizes permanent regulations. Senator Cory Booker and Senator John Hoeven presented this bill to prevent the U.S. from falling behind this quickly growing industry. Booker said in a statement, "There is so much potential that can be unlocked if we lay the proper framework to support innovation in unmanned aircraft systems. But right now, the U.S. is failing behind other countries because we lack rules for the safe operation of commercial UAS technology." Booker and Hoeven believe that commercial UAS operation could yield improvements in crop production, emergency services, and environmentally-friendly delivery of packages.

Under the proposed bill, small commercial UAS operators would be permitted to operate a UAS without an FAA certificate as long as the drone is insured and registered. Additionally, UAS operators would need to pass an aeronautical knowledge test and conduct a demonstration flight at one of the FAA testing centers in the U.S. While the bill seeks to expand commercial UAS operation, it does include some restrictions as well. Under the proposed bill, operators could only fly drones to a maximum height of 500 feet, during the daytime hours only, within the operator's line of sight, and outside of controlled airspace. An operator could face a civil action if he or she does not follow these strict requirements.

The proposed bill also seeks to create a new FAA deputy administration position called a "associate administrator for unmanned aircraft" which would exclusively handle the integration and oversight of UAS into U.S. airspace. We will track the bill to see if it takes off.

– Kathryn M. Sylvia

Maryland Governor Signs Drone Regulation Bill Into Law

On May 13, 2015, Maryland Governor, Larry Hogan, signed the Unmanned Aircraft Systems (UAS) Research, Development, Regulation and Privacy Act of 2015 into law. This new Maryland state drone Act gives the state government the exclusive power to regulate drone usage, and preempts municipalities and counties from supplying their own ordinances. The Act also requires Maryland's aviation administration, police and economic development department to research the "benefits and concerns" related to drone use, and propose ways in which drones can be used in authorized, safe ways. The research must also determine "the benefits [of drone use], including job creation, a cleaner environment, positive economic impacts, increased public safety and enhanced efficiencies." The results of this research are to be presented to Maryland state officials by the end of 2018.

This new law will take effect on July 1, 2015. This will not affect the Federal rules over UAS operation. We are likely to see more states follow Maryland's lead.

– Kathryn M. Sylvia

Florida Drone Bill Passed Into Law, More Concerns Raised About its Restrictions

At the end of April, we posted on the passing of S.B. 766 through the Florida State legislature, and now on May 14, 2015, Governor Rick Scott signed into law the Freedom from Unwarranted Surveillance Act, in the State of Florida. However, with the passing of this law, it could result in an increase in litigation

against insurance and construction companies that use drones for aerial surveying, and lead to First Amendment concerns for news media organizations. While this law is supposed to better protect Florida's citizens from unwanted intrusion into their homes, prohibiting "a person, a state agency or a political subdivision from using a drone to capture an image of privately owned real property or of the owner, tenant, occupant, invitee or licensee of such property with the intent to conduct surveillance without his or her written consent if a reasonable expectation of privacy exists," it could cause problems for companies legally using drones who might accidentally capture an image of a person in another dwelling while surveying damage from a hurricane or surveying a construction site. However, many of these concerns are hypothetical until the Federal Aviation Administration (FAA) publishes regulations that allow companies a bit more ease in obtaining licenses to fly these type of privately operated drones. We will keep watching state activity in this area and keep you updated on FAA regulation progress.

– Kathryn M. Sylvia

HEALTH INFORMATION PRIVACY

Healthcare Organizations not Immune from Criminal Attacks on Sensitive Information

This month, the Ponemon Institute released its *Fifth Annual Benchmark Study on Privacy & Security of Healthcare Data* and its findings are generating a good deal of attention. In the past, the Study has found that most data breaches in healthcare organizations were caused by lost or stolen devices or due to employee inattention, mistake or error. Publicized breaches involved improperly disposing of sensitive information or leaving a laptop or phone in the trunk or backseat of a taxi. To address these situations, healthcare organizations adopted "best practices" policies and procedures around employee education and awareness for devices, passwords and patient data.

According to the most recent Study, there has been a shift in the cause of data breaches in healthcare organizations. Today, the primary cause is from criminal attacks. The Study describes a criminal attack as a "deliberate attempt to gain unauthorized access to sensitive information." This shift in the cause of a data breach has occurred over time, with criminal attacks increasing 125 % over the last five years. However, the Study suggests that the situation will get worse before it improves, because most organizations have not taken steps to safeguard patient data against criminal threats due to lack of money, attention or other resources. Moreover, because of the lack of resources, many organizations express real concern about even being able to detect data security incidents as they are occurring or after they have occurred.

The Study also found that data security incidents are on the rise in healthcare organizations, as they are in other industries.

– Kathleen M. Porter

Comingling of Employee and Patient Data Compromises Employer's HIPAA Defense to Employee's Claim of Discharge for Union Activity

An administrative law judge (ALJ) of the National Labor Relations Board has concluded that a health care employer's use of its medical records software to store employee contact information allowed an employee to access that software for the purpose of sharing personal information about other employees with an outside union organizer. *Rocky Mountain Eye Center*, P.C., Case #'s 19-CA-134567, 19-CA-137315 (Laws, ALJ) (May 6, 2015).

The case arose out of the Rocky Mountain Eye Center's discharge of an employee who had accessed and distributed the names and personal phone numbers, including mobile phone numbers of 17 employees. The Employer had maintained that information in the same software system that it used to store information about patients.

The ALJ found that employees and supervisors accessed the system to obtain employee contact information for both work-related reasons (last-minute schedule changes) and personal reasons (after-work gatherings). The ALJ also found that that the employer had trained employees to input their data into that system, even if they were not also a patient, so that if anyone needed to contact them, they could look it up there.

The Employer argued that the employee's actions violated HIPAA. It even self- reported the alleged violations to the Department of Health and Human Services, Office of Civil Rights. The Board's General Counsel argued that "permitting use of a patient records system to store non-medical information about employees, whether patients or not, would permit HIPAA-covered employers to thwart the [National Labor Relations] Act in the guise of HIPAA compliance." The ALJ agreed with the General Counsel and concluded that the Employer's "comingling of employee and patient data in [the patient records system], along with its training instructions to employees and its practices [. . .] preclude an legitimate defense that . . . accessing the system to obtain employee phone numbers warranted discipline as a HIPAA violation."

This case not only highlights the General Counsel of Board's heightened attention to overly broad confidentiality policies, but also indicates the Board's unwillingness to yield blindly to confidentiality requirements found in other federal laws, e.g. HIPAA. In light of this decision, health care employer's may wish to review how they use their electronic records systems, as well as their confidentiality policies surrounding those systems.

– Natale V. Di Natale

CMS Issues Meaningful Use Stage 3 Proposed Rule

On March 30, 2015, the Centers for Medicare & Medicaid Services (CMS) published a proposed rule (Proposed Rule) setting forth meaningful use criteria for Stage 3 of the Medicare and Medicaid Electronic Health Record Incentive Programs (EHR Incentive Programs). CMS intends for Stage 3 to be the final stage of the EHR Incentive Programs, and as a result the Proposed Rule seeks to implement a single set of meaningful use objectives and measures designed to promote best practices and continued improvement in health outcomes. The Proposed Rule also incentivizes interoperability of health information technology and reduces the reporting burden on EHR Incentive Program providers by transitioning nearly all such providers to a calendar year reporting schedule.

The Proposed Rule sets forth eight objectives intended to (i) align Stage 3's meaningful use requirements with national health care quality improvement efforts; (ii) promote interoperability and health information exchange; and (iii) focus on CMS's three-part aim of reducing health care cost, improving health care access, and improving health care quality. Stage 3 meaningful use objectives include the following:

1. Protect Patient Information
2. Electronic Prescribing
3. Clinical Decision Support
4. Computerized Provider Order Entry
5. Patient Electronic Access to Health Information
6. Coordination of Care through Patient Engagement
7. Health Information Exchange
8. Public Health and Clinical Data Registry Reporting

CMS proposes to make compliance with the Stage 3 meaningful use criteria optional in 2017 and mandatory in 2018. CMS has solicited comments regarding the Proposed Rule, and will consider all comments received on or before May 29, 2015.

For in-depth analysis of all aspects of Stage 3 meaningful use criteria for the EHR Incentive Programs, please see this *Pulse* article from Robinson+Cole's Health Law Group.

– Conor O. Duffy

To get more thoughtful and timely discussions of legal news and perspectives on various issues relating to data privacy and security, subscribe to our *Data Privacy and Security Insider* blog by e-mail or by RSS feed.

We welcome your feedback and ideas on topics you'd like us to cover. We also encourage you to share

this *Insider* and the blog with anyone you think would find it useful.

If you have any questions, please reach out to your contact at Robinson+Cole or Linn F. Freedman, chair of our Data Privacy and Security Team.

Boston | Hartford | New York | Providence | Stamford | Albany | Los Angeles | Miami | New London | rc.com

---