Federal Bar Association
Labor and Employment Law Section
Winter 2017

The Labouring Oar

Message from the Chair

By Corie Tarara

The Labor and Employment Section is busy as ever, and we're excited to share with you several upcoming opportunities to get involved and meet up with your colleagues. Our 7th Biennial Labor and Employment Law Conference is being held March 9-10 at the Hilton Palacio Del Rio in San Antonio, Texas. We are excited to announce our keynote speaker is EEOC Commissioner Charlotte A. Burrows. In addition to Commissioner Burrows, we have a terrific lineup of speakers from private firms across the nation, the EEOC, the US Bankruptcy Court for the Western District of Texas, the DOL Veteran's Employment and Training Service, the U.S. District Court for the Western District of Texas (Austin and San Antonio), A'viands, Noodles & Company, Potbelly Sandwich Works, Lifetouch, the U.S. Department of Justice, the NLRB and the Council on American-Islamic Relations. Simply, there is something for everyone—and a wealth of knowledge to be shared and networking connections to be made. We also have sponsorships available by contacting Heather Gaskins at hgaskins@federalbar.org and would be appreciative of those willing to sponsor this great event.

In addition to the conference, the Section continues to bring our traveling half-day CLE, "Employment Law in a Nutshell," to Chapters around the nation and had successful presentations in San Diego and Phoenix, with San Juan (January 2017) and Omaha (Feb. 17) to follow. Thank you to Brian Rochel and Phil Kitzer for continuing to organize and set up these events, and to our speakers the Hon. Betsy Chestney (Western District of Texas, San Antonio Division), and Brett Strand (3M). Further, we continue to publish the monthly Case Circuit Updates, which we hope you all enjoy the new electronic format – thank you to Judge Chestney and Caitlin Andersen for their efforts with that publication. If you'd like to contribute to the monthly update or The Labouring Oar, we encourage you to reach out to them – authors are always appreciated.

Finally, I want to thank all of the Board and Committee members for their tireless work, and believe it is because of them that our Section remains the active Section that it is. We work hard to make sure the Section continues to provide top-notch services to its members. If you'd like to get involved in any way, please reach out to me or any of the Board or Committee members. Hope to see you all in March! ■

A Look at What's Inside

"Game Over for the New Overtime Rule?" 3

L&E Section's "Traveling CLE" Set to Continue in 2017 4

Barbarians at the gate? Data security concerns for the employer and counsel 5

A Membership Perk: Monthly Circuit Updates 8

2016 OSHA Overview 8

New Members 10

The Labouring Oar is published by the Federal Bar Association Labor and Employment Law Section, 1220 N. Fillmore St., Suite 444, Arlington, VA 22201, (571) 481-9100, (571) 481-9090 (fax). ISSN 1080-1316.

Barbarians at the gate? Data security concerns for the employer and counsel

By Andrew J. Broadaway

If you or your clients aren't worried about it, you probably should be. *Hacking. Data breach. Data theft. Ransomware.* I know what some of you are thinking: 'Oh, come on—we employment lawyers don't need to be concerned with this too, right? We have enough on our plates keeping up with multi-state and federal employment laws. That's a job for IT departments and compliance counsel!' I'm here to remind you: not necessarily.

With the now-constant headlines reporting state-sponsored hacking, big-business data breaches resulting in the loss of millions of dollars and consumer trust, and individuals' and businesses' vital data being hijacked and held for ransom, you would be forgiven for thinking maybe you and your clients should go back to keeping paper files and corresponding via carrier pigeon. With all of this bad news, data security experts' oft-quoted maxim now seems truer than ever—it's not a matter of "if" you or your clients will suffer some sort of data incident, but "when." At the risk of sounding alarmist, the past several years have shown such incidents occurring, or at least being discovered, at an ever-increasing rate. And, despite promises of our fully digital future, there appears to be no ultimate technical solution in sight. This all suggests that data security and breach response will be responsible for driving up business costs, legal expenditures, and IT budgets for the foreseeable future.

Of course, many of you are already aware of the risks involved with our Internet-connected world. And many of you have sophisticated clients with technological and administrative safeguards in place to manage their risks. Maybe some of your clients have robust incident-response plans and have consulted with advisors trained in preventing and dealing with data incidents. Perhaps even some of your clients have weathered such incidents, with or without your guidance. However, I am certain that some of you represent small-to-medium employers who feel like they do not face much risk from cyber threats. Therefore, they cannot justify the expense of addressing those supposedly distant risks. Or maybe you represent a company that, correctly, believes it does not deal in "data" in the traditional sense. Because the client does not process payments or deal directly with consumers' information, it feels unlikely to be the target of a cyber-attack or at risk for a data incident.

Employers Face Significant Data Risks Too, Even If The Business Is Not Data-Centric

Quick poll: how many of your clients' businesses are not connected to the Internet? OK. Now, how many of your clients' employees never access company computer systems in any way? If you raised your hand both times, you can probably stop reading. For the rest of you, it is important to counsel your clients regarding this basic truth: employee data, meaning data the employer collects and maintains about its own employees, is constantly at risk of breach and disclosure, from both external and internal sources. That's right. A disgruntled employee can do even more damage than an external hacker, given that person's knowledge of your systems. Disclosure of employee information, regardless of its source, carries legal risk similar to, if not worse than, the breach of customer data. The data an employer collects about its employees is necessarily the most personal in nature. HR departments maintain files that might include health information, financial account information, social security numbers, driver's license numbers, tax information, and addresses. Moreover, the company likely has at least some of that information on an employee's spouse or children.

All of that private information is like gold to hackers and criminals, and it is equally sought after. And, if disclosed, employee data can have more serious long-term impact that a stolen credit card or PIN number. Whereas fraudulent charges can often be quickly remedied by a card issuer, identity theft lasts forever (or at least feels like it). Therefore, if employee data is handled improperly or is inadequately safeguarded, or if that data is disclosed or stolen, an employer could have big problems. Moreover, if the breach, once discovered, is not handled in compliance with state—and even international—laws, the problems could be magnified. At worst, employees could bring a class-action lawsuit and employers could be on the hook for penalties, damages, and public notoriety—and not the good kind.

A Recent Example Of Employee Data Breach Resulting In Litigation

That appears to be the situation Sprouts Farmers Market is facing in a recently filed series of lawsuits. The cases, now consolidated and pending before U.S. District Judge Douglas Rayes in the District of Arizona *(see IN RE: Sprouts Farmers Market Incorporated Employee Data Security Breach Litigation,* 2:16-md-02731), feature current and former employees of Sprouts who allege that their personal identifying information ("PII") was accessed, stolen, and used without their authorization. The proposed class consists of more than 21,000 employees who are alleged to have had their full names, addresses, social security numbers, wages, and tax withholdings improperly disclosed. Plaintiffs allege that a Sprouts employee emailed unencrypted W-2 statements for all employees to an unknown person. The disclosing employee is alleged to have fallen victim to a phishing scam, believing that he or she was responding to a legitimate email request from a Sprouts executive. Further allegations detail a litany of horribles resulting from the disclosure of the PII: identity theft, credit reporting problems, tax fraud and refund theft, medical fraud, and, of course, resulting economic and noneconomic damages. The lawsuits allege that Sprouts failed to abide by the breach notification laws of most states, including California and Arizona. Additionally, Sprouts stands accused of acting negligently for how the company stored and maintained its employee records and how it disclosed the W-2 forms.

Regardless of the outcome of this particular or other, similar litigation, one message is clear: the risk to employers is real, and the consequences are costly. It is easy to look at cases like *Sprouts* and think 'Wow, that's bad, but it would never happen to me or my client.' Assuredly, basic safeguards like encrypting and password-protecting sensitive data might have helped prevent the particular outcome for Sprouts. As might security-awareness training for employees or robust email-filtering tech-

nology to block phishing attempts in the first place. Companies of all sizes should definitely devote appropriate resources to preventive measures, both technological and administrative. However, no amount of technology or training will prevent all incidents. The criminals are almost always innovating ahead of the technological curve, and training relies on imperfect people always remembering to be perfect.

At a recent CLE event an experienced attorney, savvy with computers and versed in current threats, detailed how he fell victim to a ransomware attack. He was busy and distracted, receiving dozens of legitimate emails that afternoon with attachments. The email in question appeared to be from someone he knew, and he was expecting an email from that sender. He clicked on the attachment instinctively and then realized, almost instantly, that it wasn't a real attachment but, instead, was a program. The software had started encrypting his files, starting with the most recent ones. After a few seconds of flailing, he had the presence of mind to unplug the computer's power cable and take the hard drive to a forensic specialist for recovery. He was lucky—he lost only a couple of weeks of work, and he did not have to pay a hacker to get years of his work product back. The point of that story, other than serving to scare me into triple checking every attachment, was that, no matter how careful you are or how much your clients trust their security systems, all it takes is a momentary lapse to suffer a data incident with lasting consequences.

What Are Employers And Their Counsel To Do?

The most important piece of advice? Have a plan. Often called an "incident-response plan," companies (and the law firms that support them) should have a written, researched, communicated, and practiced plan in place well before any incident occurs. The plan can be simple or elaborate, depending upon the complexity of the organization and the amount and type of data that it keeps. Each employer's plan should start by cataloging all types of sensitive data maintained by the organization, who uses it, who has access to it, how it is stored, where copies of such data might exist, and the safeguards in place to protect it.

Identify Your Response Teams

A response plan should also designate internal and external crisis teams. Internal teams should be small, agile, and well trained—familiar with the IT systems and data in question. They should also include, or at least directly report to, senior management. Keeping the initial stages of incident investigation and response absolutely confidential is critical; sometimes incidents are not as serious as they initially appear, and unsubstantiated or false rumors of a data breach can be extremely damaging to company morale and reputation.

External teams should likely include counsel or someone well-versed in privacy and breach reporting, assuming those are not resident in-house. In addition, companies should consider ongoing relationships with crisis-management and forensics vendors as part of their plan. Vendor contracts should be signed well in advance of any incident, and the team dynamics and professional relationships should be well-established. There is nothing worse than having to scramble to review vendor contracts and coordinate unknown personnel while the breach-notification timeline is ticking down, or even worse, if the breach is still actively happening.

Flexibility Is Key

Another vital thing to remember: make sure your plan is flexible enough to deal with small incidents, as well as large ones. Most companies' incident-response plans seem to focus almost exclusively on catastrophic data breach—the ones that make the headlines. Certainly, large-scale hacks originating from outside the company do happen. Just ask Sprouts, the U.S. Office of Personnel Management, and SnapChat, to name a few. However, more realistic, and more frequent, are smaller-scale internal incidents. You get a report that one of your client's HR generalists has lost a thumb drive containing a spreadsheet compiling sensitive employee data. The plan should cover that. A review of a recently terminated employee's computer activity shows that he was emailing himself attachments suspected to contain protected data. Your plan should cover that too.

Practice and Communicate

Almost as important as having a plan is practicing the plan. This may involve something as simple as tabletop strategy sessions going over the aspects of the plan with all key personnel. Or it could involve a full-scale simulated incident where only very few of the players know that it is a drill. Nothing will identify shortcomings in an incident-response plan quite like a realistic simulation. Often, executing certain aspects of a data-incident response are time-critical. Identifying bottlenecks or missing communication channels before there is an actual event can sometimes mean the difference between timely remediation or blown breach-notification deadlines.

It may seem obvious, but a crucial precursor to practicing the plan is making sure that it is well documented and communicated to crucial team members, including their backups. But equally vital is making sure that rank and file personnel are aware that an incident plan exists and that they know to report an incident when it happens. Returning to the lost HR thumb drive example: if the HR generalist is not aware that he needs to report the loss of sensitive HR data, it might go unnoticed until too late. If the HR generalist reports the loss to his manager, but the manager does not report the incident up the chain to activate the incident-response protocol, the company may have suffered a report-triggering breach, but failed to timely act and notify necessary parties.

Revisit, Revise, Repeat

Finally, incident-response plans are not intended to be static documents. Changes in management, personnel, reporting, IT infrastructure, vendors, or HR practices may all trigger a need to revisit and revise the plan. New attack vectors or technological vulnerabilities may be discovered that require a different approach to your incident response. Also, as will be discussed below, your jurisdiction's breach notification laws may change, rendering certain aspects of your plan obsolete. Make sure that your client knows that they should be revisiting their incident-response plan with regularity, optimally in conjunction with a practice run or whenever the

company undergoes significant operational changes.

Breach Notification for Employers

A full discussion of data breach notification laws and how they differ between various states and countries is far beyond the scope of this article. But as the *Sprouts* cases demonstrate, incomplete or untimely compliance with applicable state notification laws can be a major source of liability. The challenges facing multi-state or multi-national employers are legion. There is no uniform approach to notification triggers, which information is required to be disclosed to affected parties, when state entities must be informed, and the timing of notification after the disclosure is discovered. Generally speaking, the United States lags behind the rest of the world when it comes to privacy regulation, so if you are advising clients with international employees, they should be prepared to comply with much stricter rules.

Expanding State Laws

Forty-seven states (all but Alabama, New Mexico, and South Dakota), the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have enacted legislation requiring private entities to notify affected individuals of security breaches involving their personally identifiable information. The legislation differs, but nearly all have provisions defining who must comply with the law, what constitutes personal information, what constitutes a breach, the requirements and timing of notice, and exemptions to the notification requirements. Recent trends show that states are amending their breach notification requirements to be broader, and require more and earlier notification. Eight states amended their breach notification laws in 2015 to add new and unique requirements. In 2016, at least 26 states have introduced or are considering security breach notification bills or resolutions, mostly amending existing legislation to expand coverage.

Inconsistencies between existing state laws and staying on top of constant amendments can create compliance nightmares for multi-state employers. For example, in October 2015, California amended its breach notification law and mandated a specific form of notice with required information and specific headings. However, other states may require different, or additional, information to be shared. Massachusetts and Rhode Island mandate that affected individuals be informed of their right to obtain a police report, but California does not. Wyoming requires that a breach disclosure specify whether law enforcement requested the affected entity to delay notification. This inconsistent approach renders a single notice form almost impossible to draft.

Know Your Triggers

Knowing what events "trigger" breach notification laws is also vital. Different categories of information may be treated differently in neighboring jurisdictions. What is considered PII in one state may not be in an adjacent state. However, as a general rule, names and associated SSN's will nearly always trigger a breach law. Also, the size of the breach and the affected number of employees may trigger different reporting requirements. Nearly half of states require reporting data breaches to the state's Attorney General; many of those mandate such disclosure regardless of the number of individuals affected. Other states require notice to state regulatory bodies or investigative entities. State involvement can lead to administrative inquires and possible fines.

Don't Delay Once You Learn Of An Incident

Breach notification deadlines are another source of inconsistency and confusion. While most states' laws provide a flexible notification deadline, typically "as soon as reasonably practicable" or "without unreasonable delay," that's not always the case. Some states already impose strict deadlines, and other states appear to be following suit. Ohio, Rhode Island, Tennessee, Vermont, Washington, and Wisconsin require notice to be delivered within 45 days of the discovery of the breach. Florida requires notice within 30 days. These deadlines are a critical part of any employer's incident-response plan, and the importance of complying with the deadlines cannot be understated.

Keep Calm And Carry On

As sobering as it is to realize the risks facing most of our clients by virtue of the sensitive employee data they all maintain, take a deep breath. All is not gloom, doom, and litigation headaches. If you and your clients plan for—and execute—appropriate protection measures and calculated responses, the inevitable data incident can be dispatched with minimal disruption to normal business. Nearly every employer faces some risk of a data breach; our HR departments could not function without collected data. However, the consequences of an incident are exacerbated by responding inappropriately or, worse, not at all. With these topics in mind, you should be able to help your clients plan for risks that some may not have even known existed.

Luckily for all of us, there are many free or inexpensive resources available to help the employer and their counsel navigate this complicated environment. Employers should also check with their insurance providers, as many are now offering policies to help offset the cost of an incident. If you or your clients face a data incident before having developed and refined a response plan, don't panic. While it is probably wise to consult with counsel familiar with breach and incident response and who can guide you in remediation, you will not be alone in dealing with these challenges. ■

Andrew J. Broadaway is an attorney specializing in labor and employment litigation and employer counseling with the Austin, Texas law firm Cornell Smith Mierl & Brutocao, LLP. He is also a Certified Information Systems Security Professional (CISSP #322890) and member of the International Association of Privacy Professionals. Andrew's previous career as an information security consultant gives him a unique perspective on the data security and privacy issues facing employers. Andrew can be reached at: abroadaway@cornellsmith.com.