VEDDERPRICE®

August 2008

Retail Industry Briefing

Data Security Breaches and Privacy Incidents

Companies have developed new ways to create, store, access, use and LOSE data. Indeed, since January 2005, the Privacy Rights Clearinghouse has reported that more than 1,000 data breaches have occurred, involving more than 220 million records. In reality, the number of actual data breaches is much higher, given that not all incidents are reported. Notably, however, in just the first quarter of 2008, 167 data breaches have been reported, involving 8.3 MM financial and consumer records. A data breach or loss can occur in a variety of ways:

- An executive loses a laptop;
- A hacker accesses a computer storage system; and
- A third party responsible for maintaining, transporting, or processing data is negligent in its handling.

As illustrated below, these breaches have left no industry untouched.

Best Buy's $54 Million Lost Laptop

Articles and reports of privacy litigation have discussed the problems and damages awards that companies face when they are the victim of security breaches involving the disclosure of customer or employee personally identifying information ("PII"). Typically, these issues arise in the context of large-scale security breaches, such as the theft of the PII of 1.3 million Monster.com users in August 2007, or the loss of computer data tapes holding the PII of credit card users. However, a recent event involving Best Buy serves as a reminder such security breach issues are not limited to large-scale breaches.

In May 2007 Raelyn Campbell left her malfunctioning one-year-old laptop at a Washington, D.C., metro area Best Buy for routine repairs under a service contract, but Best Buy never returned the laptop. For months, Ms. Campbell sought information regarding the whereabouts of her computer, and for months, Best Buy equivocated. Eventually, Best Buy confirmed what Ms. Campbell already suspected: That it had lost her computer.

With a corporation as big as Best Buy, which has over 1,150 stores in the United States, Puerto Rico, Canada and China, thefts are inevitable and equipment will occasionally be lost. Thus, at first blush, the loss of a single laptop may not seem like a big deal. However, when companies do not have a predetermined policy in place for responding to such incidents, they can unwittingly subject themselves to far more civil liability and negative publicity than one might expect.

On November 16, 2007, Ms. Campbell filed a lawsuit against Best Buy in Washington, D.C., Superior Court seeking

in this issue...

$54 million in damages. In her complaint, Ms. Campbell alleges that Geeksquad (Best Buy's computer service subsidiary) and Best Buy customer service employees created a false record of her computer within their system, and they lied about its repair status and location.

Ms. Campbell also alleges that, in losing her computer, Best Buy put her personal identification information at risk, as the computer contained information such as her social security number, driver's license number and credit card information. Ms. Campbell additionally alleges that Best Buy compounded the problem by waiting months before advising her that the computer was missing, and that her personal information might be in the hands of others. More specifically, Ms. Campbell is alleging that Best Buy violated the Washington, D.C., Consumer Protection Procedures Act, D.C. Code § 28-3901 et seq., and the Washington, D.C., Consumer Personal Information Security Breach Notification Act, D.C. Code § 28-3801 et seq.

Best Buy's actions as characterized by Ms. Campbell could constitute unlawful trade practices under the Consumer Protection Procedures Act if a court were to find that Best Buy

- made misrepresentations as to a material fact that had tendencies to mislead;
- failed to state material facts if such failure tended to mislead;
- falsely stated or represented that repairs, alterations, modifications, or servicing had been made and payment received for such, when they had not been made; or,
- represented that the subject of the transaction had been supplied in accordance with a previous representation, when it had not.

D.C. Code § 28-3904 (e), (f), (p), and (u).

Perhaps even more problematic for Best Buy are its alleged violations of the Consumer Personal Information Security Breach Notification Act, the stated purpose of which is to "ensure that consumers are notified when electronically-stored personal information is compromised in a way that increases the risk of identity theft, to create a private right of action for consumers harmed by a violation of the notification requirement, and to provide for enforcement by the Attorney General." Because it is perfectly reasonable to assume that the type of personal information identified under the Act, such as social security numbers, driver's license numbers or credit card information would be stored on a customer's personal computer, there is a strong likelihood that the Act imposed upon Best Buy a duty to notify Ms. Campbell immediately upon discovering that her computer was missing. Specifically, § 28-3852(b) requires that "[a]ny person or entity who maintains, handles, or otherwise possesses computerized or other electronic data that includes personal information that the person or entity does not own shall notify the owner or licensee of the information of any breach of the security of the system in the most expedient time possible following discovery." D.C. Code § 28-3852(a).

Beyond the cost of defending such a suit and any adverse judgment for actual damages, the Act also authorizes a plaintiff to recover "the costs of the action and reasonable attorney's fees." D.C. Code § 28-3853(a).

While personal information security breach–related issues generally arise when large databases that are maintained by companies, containing the personal information of thousands of people, are compromised, this case demonstrates the need to be prepared even for a breach involving a single consumer. Had Best Buy had a predetermined policy in place in advance of this incident (or followed any pre-existing policy it may have had in place) it might have forestalled any potential liability. In fact, the Consumer Personal Information Security Breach Notification Act specifically protects a business that has such a policy in place:

> a person or business that maintains its own notification procedures

> as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this subchapter shall be deemed to be in compliance with the notification requirements of this section if the person or business provides notice, in accordance with its policies, reasonably calculated to give actual notice to persons to whom notice is otherwise required to be given under this subchapter.

D.C. Code § 28-3852(e).

In addition to protecting themselves by enacting a company policy on security breach notification procedures, retailers can also protect themselves by taking steps to lessen the likelihood of a security breach in the first instance.

Although it is unlikely Ms. Campbell will ever receive the $54 million she seeks, Best Buy has opened itself up to the possibility of a judgment that would be significant to most companies, not to mention damage to its reputation. Ms. Campbell has already appeared on the *Today Show*, and her story has been reported by numerous media outlets. This case thus highlights the need for companies handling sensitive personal information to maintain predetermined and up-to-date plans in the event of a security breach, and to remember that such plans should be followed even where only a single person's personal identification information is at issue.

As illustrated above, all companies must take proactive steps to mitigate the likelihood of a privacy incident. Indeed, 42 States (and counting) have enacted data security breach notification laws, so if one occurs, your company must understand what constitutes a violation, at what point a notice of data security breach is required, and whether it must alert Federal, State or local authorities. Additionally, your company should strive to:

- Develop data security policies and response protocols in the event of a data security breach;
- Involve your company's compliance, human resources, information security and legal teams in the development of your company's data security policies and response protocols;
- Understand how data security notification laws will impact your response and guide your company's policies;
- Develop a policy on employee blogging, which should minimize the risk of employees' defaming fellow employees, divulging proprietary and confidential information, and violating other company policies;
- Identify patterns and activities that present "red flags" indicating possible identity theft;
- Respond appropriately and swiftly, should a "red flag" arise;
- Review agreements with vendors and third parties who maintain PII regarding your employees and customers; and
- Document steps taken to respond to a data security event, in order to demonstrate compliance with applicable laws and regulations. ■

Immigration Raids– Tips for Avoiding Corporate Liability

Nearly every week, the U.S. Department of Homeland Security's Immigration & Customs Enforcement ("ICE") issues a press release announcing another worksite immigration raid. ICE has dramatically changed its enforcement of the immigration laws. Rather than relying on the traditional use of administrative fines for I-9 violations, ICE is bringing criminal charges against employers and seizing their "illegally derived" assets.

Last fiscal year, this new approach resulted in 863 criminal arrests and over 4,000 administrative workplace arrests. As recently as July 21, 2008, two top executives for a McDonald's franchisee that owns 11 McDonald's restaurants and the corporation itself pleaded guilty to federal

felony immigration offenses, and agreed to pay a fine of $1 million. Also in July 2008, the president of a Cincinnati-area company was sentenced to eight months in prison for harboring illegal aliens "for commercial advantage and private financial gain." The company was also sentenced to two years' probation and ordered to pay $2 million in fines.

What triggers a government investigation into your worksite? Governmental investigations often arise in strange and unassuming situations. For instance, a disgruntled former employee or a competitor may relay information to ICE. This might include information or allegations relating to the hiring of undocumented workers, or the actions of recruiters in acknowledging the existence of fraudulent documents. Recent raids have been triggered by Social Security no-match letters, even when employers are enrolled in government programs that check social security numbers and identities. A Wage and Hour audit may result in the Department of Labor contacting ICE to discuss irregularities in a company's I-9 records.

Fortunately, guidelines exist to help employers avoid both prosecution and severe sanctions. The United States Sentencing Commission's federal sentencing guidelines for organizations describe a "Culpability Score." Pursuant to the guidelines, an effective compliance and ethics program is one of the mitigating factors that can reduce an organization's punishment for criminal immigration violations. Whether a corporation will be indicted will depend on a number of factors listed in the Department of Justice "McNulty" memo, including the existence of a *preexisting* compliance program, as well as remedial actions such as replacement of responsible management and termination of wrongdoers.

It is nearly impossible (and is not legally required) for an employer to confirm that 100% of its workforce is lawful. Fraudulent documents abound, and careless employers can unknowingly hire workers without appropriate documentation. An immigration compliance program is one of the few ways that employers can exercise some control over their civil and criminal liability in immigration matters. In order to avoid liability for immigration violations, it is critical that employers understand, implement, execute—and document their execution of—internal immigration compliance programs that encourage due diligence at all levels in the organization.

What are the key elements to include in a corporate immigration compliance policy?

1. The policy language should be clear and understandable, and should plainly state that all employees are to comply with relevant federal, state and local immigration laws, and behave at all times in an ethical manner.
2. The policy should require that a compliance officer be selected who will be ultimately responsible for ensuring that the company and its employees and agents understand the laws and comply with the policy.
3. The policy should require regular training programs for all levels of employees—from senior management to receptionists.
4. A monitoring system should be established to measure compliance with the policy and its effectiveness. Ramifications for violation of the policy should be clearly outlined and applied uniformly.
5. In consultation with litigation counsel, a procedure should be established for dealing with government visits, audits, investigations and raids. This procedure should be communicated to "front line" employees, including security guards, receptionists, etc.
6. Ensure that the company provides post-audit and post-raid training for all involved individuals to further protect the company from follow-up actions by

the government after a raid or audit occurs.

7. The company should develop an internal mechanism to address post-hire and initial I-9 completion issues, including instances in which third-parties (for instance, clients or subcontractors) provide information indicating that an employee is not authorized to work.
8. The policy should include clear guidelines regarding I-9 compliance. This section of the policy should require regular I-9 training; ensure that I-9 documents are included in the company's Document Retention Schedule; and schedule regular internal I-9 audits to analyze potential risks and mitigate fines and damages prior to any government action.
9. The company should ensure that its legal department or outside counsel reviews subcontractor agreements involving provision of temporary labor or services performed on company property. These agreements should include representations and warranties that the subcontractor(s) will comply with all federal, state and local immigration laws. Employers may also desire to include a provision that subcontractors will indemnify the company for any damages and legal fees the company incurs, should they fail to comply with applicable immigration laws.
10. Establish a decision-making process through which the company determines whether it will sponsor an employee for lawful permanent residence or require the employee to bear immigration-related costs (when legally permitted). The company can avoid the appearance of discrimination or disparate impact by setting up a process that treats employees consistently, regardless of their national origin. Multinational companies should also establish a global immigration plan. Prior to the transfer of employees, it should determine which local immigration laws apply and decide which costs the company will pay.

Clearly, in light of increased enforcement of both civil and criminal immigration laws, employers should ensure that their codes of conduct and immigration compliance policies are capable of providing maximum protection for their organizations. ■

Tax Risk Related to Independent Contractors

Independent contractors are a growing segment of the retail workforce. Lower costs, reduced liability, and hiring flexibility are just a few reasons that retailers find hiring independent contractors to be so attractive. While these benefits are alluring, retailers need to be aware of the risks involved when engaging independent contractors.

The most significant potential liability of worker misclassification is back federal, state and local payroll tax withholding (e.g., FICA and income tax). The IRS has made reviewing employee misclassification a priority when conducting audits. Other potential liabilities include overtime, benefits, and unemployment compensation. Often, the way the IRS becomes aware of misclassification issues is through communication with state unemployment or revenue agencies, who regularly share information with the IRS on employee misclassification.

Recently, a number of retailers, as well as other organizations, have paid the price for wrongly classifying workers as independent contractors. Several national supermarkets have settled lawsuits for several million dollars, where workers,

employed by subcontractors alleged that the retailers were responsible for overtime and other Fair Labor Standards Act violations, under a joint employer theory. Retailers had argued that the workers were contractors and not employees. Most recently, the IRS opened many eyes when it hit FedEx with $319 million in federal tax liability for 2002 alone (the IRS is still auditing other years) because FedEx classified the delivery drivers as independent contractors, while the IRS found them to be employees.

The lesson from these cases is clear—retailers interested in hiring independent contractors must be cautious. Courts and regulatory agencies use numerous legal tests to determine whether a worker qualifies as an independent contractor or is an employee. Any test is fact-intensive and inherently subjective. However, the most critical test is the right of the employer to control the work being done.

In short, the financial impact of misclassifying workers can be enormous. Accordingly, retailers should closely scrutinize any work situation before classifying a worker as an independent contractor. ■

Retail Industry Service Team Group Members

Timothy J. Carroll (Litigation/eDiscovery)
Chair, Retail Industry Service Team
312-609-7709
tcarroll@vedderprice.com

Eric A. Berg (Leasing)
312-609-7635
eberg@vedderprice.com

William J. Bettman (Corporate and M&A)
312-609-7776
wbettman@vedderprice.com

Gabrielle M. Buckley (Immigration)
312-609-7626
gbuckley@vedderprice.com

Matthew F. Carmody (Franchise)
312-609-7798
mcarmody@vedderprice.com

Danielle Meltzer Cassel (Leasing)
312-609-7962
dcassel@vedderprice.com

Christopher T. Collins (Employee Benefits)
312-609-7706
ccollins@vedderprice.com

David P. Dorner (Taxation)
312-609-7764
ddorner@vedderprice.com

Aaron R. Gelb (Employment)
312-609-7844
agelb@vedderprice.com

Michael L. Igoe (Real Estate)
312-609-7555
migoe@vedderprice.com

P. Michelle Jacobson (Immigration)
312-609-7761
mjacobson@vedderprice.com

William J. Lewis (Leasing)
312-609-7930
wlewis@vedderprice.com

Margo Wolf O'Donnell (Litigation/Employment)
312-609-7609
modonnell@vedderprice.com

Bruce A. Radke (Litigation/Records Management)
312-609-7689
bradke@vedderprice.com

Robert S. Rigg (Intellectual Property)
312-609-7766
rrigg@vedderprice.com

Timothy M. Schank (Construction)
312-609-7585
tschank@vedderprice.com

Kelly A. Starr (Employee Benefits/Executive Compensation)
312-609-7768
kstarr@vedderprice.com

Michael J. Waters (Privacy Litigation)
312-609-7726
mwaters@vedderprice.com

Jonathan A. Wexler (Employment)
212-407-7732
jwexler@vedderprice.com

Thomas M. Wilde (Employment)
312-609-7821
twilde@vedderprice.com

Pearl A. Zager (Real Estate)
312-609-7548
pzager@vedderprice.com

VEDDERPRICE®

222 NORTH LASALLE STREET
CHICAGO, ILLINOIS 60601
312-609-7500 FAX: 312-609-5005

1633 BROADWAY, 47th FLOOR
NEW YORK, NEW YORK 10019
212-407-7700 FAX: 212-407-7799

875 15th STREET NW, SUITE 725
WASHINGTON, D.C. 20005
202-312-3320 FAX: 202-312-3322

www.vedderprice.com

Retail Industry Briefing

The Vedder Price Retail Industry Service Team ("RIST") is dedicated to providing comprehensive, multi-disciplinary legal services to our retail industry clients that enhance their business, productivity and profitability while reducing their legal exposure. Members of the Retail Industry Service Team provide counsel and advice in key legal areas, such as labor and employment; corporate and tax strategies; real estate financing & development; brand protection; immigration; e-commerce; and franchise and distribution dispute resolution.

Vedder Price works with different types of retail industry clients, providing a full suite of transactional, litigation and regulatory services tailored to each client's unique needs.

We welcome your suggestions and comments. Please contact **Timothy J. Carroll** in Chicago at 312-609-7709.

About Vedder Price

Vedder Price P.C. is a national, business-oriented law firm with over 260 attorneys in Chicago, New York and Washington, D.C. The firm combines broad, diversified legal experience with particular strengths in labor and employment law, occupational safety and health, general litigation, corporate and business law, commercial finance, financial institutions, environmental law, securities, investment management, tax, real estate, intellectual property, estate planning and administration, health care, trade and professional association, and not-for-profit.

The *Retail Industry Briefing* is published periodically by the law firm of Vedder Price P.C. It is intended to keep our clients and interested parties generally informed about developments in the financial services industry. It is not a substitute for professional advice. For purposed of the New York State Bar Rules, this newsletter may be considered ATTORNEY ADVERTISING. Prior results do not guarantee a similar outcome.