BALCH & BINGHAM LLP

B&B REVIEW

Business Litigation Practice Group

What's Inside . . .

For Further Information Contact . . .

Gregory C. Cook
205-226-3426
gcook@balch.com

Will Hill Tankersley, Jr.
205-226-3424
wtankers@balch.com

Address Change . . .

If you no longer wish to receive this update or have an address change, please contact:

Nora Yardley
205-226-3476
nyardley@balch.com

LIABILITY FOR CUSTOMER DATA ON EMPLOYEE LAPTOPS

INTRODUCTION

Security for customer data is becoming a larger focus of media, regulators, and customers every day. Some states have passed draconian notice and liability statutes for the loss of consumer data, the Federal Trade Commission has taken action against certain corporations who have compromised consumer data (for instance, the recent ChoicePoint settlement for $15 Million) and the courts are finally getting into the act. See Bell v. Michigan Council 25 of AFSCME, 2005 WL 356306 (Mich.App. Feb. 15, 2005) (union had special relationship with members and therefore duty to predict personal information). Several recent examples have involved laptop thefts, such as the Fidelity Investment's employee computer in mid-March, 2006 (containing 196,000 Social Security Numbers and associated personal information). Perhaps the most well-known breach involved the recent data compromise at VA. The Privacy Rights Clearinghouse, a consumer group, lists 27 incidents involving such thefts in the last 13 months. See generally Jeniffer Levitz & John Hechinger, Laptops Prove Weakest Link in Data Security, Wall St.J., March 24, 2006, at B1.

THE GUIN LITIGATION

In Guin v. Brazos Higher Education Service Corp., Inc., 2006 WL 288483 (D. Minn., Feb. 7, 2006), the federal court refused to impose liability upon a financial institution for the loss of consumer data. There, a loan analyst brought home sensitive, unencrypted personal data on a laptop. His home was burglarized and the laptop stolen. Consumers sued. The financial institution argued on summary judgment that neither the employee nor the company had been negligent, and the court agreed.

Importantly, however, the court accepted the plaintiff's argument that the company owed the student (plaintiff) a duty of care for protecting such data, and at the basis of that duty was the Gramm-Leach-Bliley (GLB) Act, 15 U.S.C. § 6801. Nevertheless, the court found that working from home is common and the burglary was not foreseeable. Furthermore, the employee followed the company's written security procedures, and that this was all that the GLB Act required.

The Guin court rejected the argument that encrypting the data was mandatory. It noted that "the GLB Act does not contain any such requirement." Instead, GLB merely requires reasonable measures to protect data -- setting up goals, not procedures. GLB does not expressly require a firewall, a password, or encryption. In fact, the entire security guidelines of GLB are hardly one page long.

The financial institution in Guin acted quickly. It notified its customers of the breach and set up an information hotline. This made the financial institution appear reasonable to the court. However, it should be noted that the students, not the financial institution, bore the cost of placing a fraud alert on their credit cards and safeguarding their financial identities.

LESSONS LEARNED

The Guin case teaches several lessons. First, simply because there is a breach of data security does not mean that the company is necessarily liable. Second, companies should have (must have) a security program that is written down, communicated to employees, targeted to specific threats against the company, and enforced. Third, while encryption is not required today, industry standards could change quickly. Future decisions will depend upon the actions of other financial institutions, state laws in the majority of the country, and new technology which may make encryption easier or a lower cost. As the price of security drops and the likelihood of data breaches rises, a future court may find failure to use encryption to be negligent. Encryption introduces an extra layer of inconvenience and training. The annoyance and inconvenience

versus the higher protection it provides is not yet valued by business.

DAMAGES REQUIREMENT

In Forbes v. Wells Fargo Bank, D. Minn., No. 05-2409 (DSD/RLE), 3/16/06), the federal court granted summary judgment on plaintiffs' negligence and breach of contract claims holding that the threat of future harm alone is insufficient to meet the damages requirement for these type of claims.

The case involved a subsidiary of Wells Fargo which hired a service provider, Regulus Integrated Solutions, to print monthly statements for home equity mortgage and student loan customers.

In October 2004, computers were stolen from the service provider that contained unencrypted customer information including names, addresses, social security numbers and account numbers. That same month, Wells Fargo notified potentially affected customers of the theft and offered informational and identity protection services.

Plaintiffs filed suit in Minnesota state court seeking class action status on behalf of all affected bank customers arguing that the time and money they spent monitoring their credit should suffice to establish damages. Wells Fargo removed the case to federal court. Under Minnesota law, plaintiffs may only recover for loss of time in terms of earning capacity or wages.

However, there was no evidence that the information on the stolen computers had been accessed or misused. Thus, the required element of intent to use the identity information of another was not met.

The court also noted that plaintiffs' expenditure of time and money was not the result of any present injury, but the anticipation of future injury that had not materialized. Because plaintiffs' injuries were solely the result of a perceived risk of future harm, the court found they had not shown any present injury or reasonably certain future injury to support damages for any alleged increased risk of harm, thus failing to establish the essential element of damages.

GENERAL LESSONS

In sum, most companies need a data security policy. Moreover, most should have a planned response to breaches of data security. This includes assessing the nature of the incident, identifying affected customers, notifying any applicable regulators, containing the breach, alerting law enforcement if necessary, and notifying customers if warranted.

Visit Our Offices . . .

1901 Sixth Avenue North
Suite 2600
Birmingham, Alabama 35203

1710 Sixth Avenue North
Birmingham, Alabama 35203

2 Dexter Avenue
Montgomery, Alabama 36104

655 Gallatin Street
Huntsville, Alabama 35801

3535 Piedmont Road
14 Piedmont Center
Atlanta, Georgia 30305

1310 Twenty-Fifth Avenue
Gulfport, Mississippi 39501

401 East Capital Street
Suite 200
Jackson, Mississippi 39201

1275 Pennsylvania Avenue, N.W.
Washington, D.C. 20004

Visit our website
www.balch.com