NEW YORK'S DATA PRIVACY GUIDE OFFERS BEST PRACTICE TIPS FOR PROTECTING PERSONAL INFORMATION AND PREVENTING IDENTITY THEFT

On November 1, 2008, the New York State Consumer Protection Board ("CPB") released a report entitled "*Business Privacy Guide: How to Handle Personal Identifiable Information and Limit the Prospects of Identity Theft*" ("Guide").[1] The CPB is New York's consumer watchdog agency, the mission of which is in part "to protect the residents of New York by publicizing unscrupulous and questionable business practices."[2] The release of this Guide signals a heightened focus on the prevention of identify theft in New York, and the possibility of increased investigations and/or prosecutions of businesses that do not adequately protect the personal information of New York consumers and employees.

Significant Risks Facing All Businesses

The possibility of identity theft raises serious and potentially costly issues for consumers and businesses alike. For example, businesses that experience a data security breach can: (1) face stiff civil penalties, (2) become the target of a class action lawsuit, and/or (3) experience significant drops in business due to public concerns about the company's ability to adequately protect consumer information. According to one reputable report, a data security breach can cost businesses an average of $192 per data subject, per incident, which can add up quickly. It is estimated that the well-known TJX data breach may end up costing the company $1.7 billion.[3] Beyond the costs of such remedial measures, one report found that almost 33% of consumers surveyed would cut ties with a company that had a data breach.[4] Given these significant financial, reputational, and legal risks, the Guide stresses that businesses need to focus on crafting a privacy policy and implementing strong data security practices that conform to applicable laws and reduce the likelihood of a data breach occurring in the first place.

---

1 The report is *available at* http://www.consumer.state.ny.us/pdf/the_new_york_business_guide_to_privacy.pdf.

2 *Id.*

3 *See* Singel, R., *Data Breach Will Cost TJX $1.7B, Security Firm Estimates*, Wired (3/30/07) (*available at* http://blog.wired.com/27bstroke6/2007/03/data_breach_wil.html).

4 *Supra n.*1 at 3, citing Ponemon Institute 2007 Annual Study: Cost of Data Breach (*available at* http://www.ponemon.org/index.html).

Key Elements of New York's Business Privacy Guide

Survey of Applicable New York Laws

The Guide provides a helpful summary of the key data privacy and data security laws in New York, including the following:

Protection of Social Security Numbers: As of January 1, 2008, New York prohibited individuals and business entities from making a Social Security number available to the public, whether intentionally or not, and from printing an individual's Social Security number on a tag or card that is required for access to a company's products or services. On the Internet, an entity cannot require an individual to transmit his or her unencrypted Social Security number or use it for access without additional authentication. Businesses must take reasonable measures to ensure that only those officers or employees with a legitimate business purpose have access to Social Security numbers. Additional provisions will become effective January 3, 2009. As of that date, Social Security numbers may no longer be embedded on a card or in a document, and anything filed for public inspection must not contain Social Security numbers without that individual's consent.[5]

Use of Credit and Debit Cards: Businesses that issue receipts acknowledging payment by credit or debit card must do so either with carbonless paper, or without issuing a separate piece of paper with a readily identifiable customer name or number. Not more than the last five digits of a credit or debit card number may appear on any receipt.[6]

Employee Information: Beginning on January 3, 2009, employers must neither post an employee's Social Security number, nor use a Social Security number on an identification badge or time card. Further, the employer cannot have Social Security numbers in files with unrestricted access, or communicate personal identifying information to the public.[7]

Notification: If a data breach occurs, New York's notification law -- the Information Security Breach and Notification Act -- requires persons and companies that conduct business in New York to notify state residents of acquisitions by unauthorized parties of "private" information. Firms that maintain, but do not own, private data are also obligated to notify the entity that owns the data that a breach has occurred, which triggers the notification obligations of the owner. The penalties for nondisclosure can range from $5,000 to $150,000.[8]

---

5 N.Y. CLS Gen Bus § 399-dd (2008).

6 N.Y. CLS Gen Bus § 520-a (2008).

7 N.Y. CLS Labor § 203-d (2008).

8 N.Y. CLS Gen Bus § 899-aa (2008); *see also* Client Memorandum, *New York Enacts Information Security Breach and Notification Act; Entities That Conduct Business in New York and Possess Computerized Data Must Comply by December 2005*, Willkie Farr & Gallagher LLP (Aug. 22, 2005).

Recommended Data Security Practices

In light of more focused attention on data security breaches both at the New York state level and at the federal level with Red Flag rules,[9] companies that conduct business in New York must take extra care in crafting a privacy policy and ensuring that personal information of customers and employees is secure. That policy should reflect the unique business practices and organizational features of a given entity and be updated frequently as the legal landscape of state and federal law changes. In general terms, each entity should at a minimum use the following guidelines:

1. Unless there is a legitimate business purpose, do not collect or retain personal information on customers or employees;

2. Minimize gathering and using Social Security numbers from individuals to limit the exposure of personal information if a security breach occurs;

3. Only authorize those officers and employees with a legitimate business purpose to access personal information;

4. If there is no reason to have personal information, do not store it in either physical or electronic form;

5. Develop safeguards to secure physical and electronic access to personal or sensitive information;

6. Train staff regularly to show that privacy protection is a priority;

7. Prepare for a data breach by taking steps to mitigate risks and reduce the company's vulnerabilities;

8. In the event of a security breach, know whom to notify;

9. Become familiar with, and consider hiring someone with expertise in, New York privacy laws and the relevant laws of any other state and/or country in which the company does business;

10. Update the company privacy policy to reflect any changes in applicable laws and developments in best practice procedures; and

11. Adopt and implement appropriate record disposal and destruction policies.

---

[9] *See* Client Memorandum, *"Red Flag" Identity Theft Rules May Have You Seeing Red: FTC Extends Compliance Deadline Because Many Companies Did Not Know That These Rules Apply to Them*, Willkie Farr & Gallagher LLP (Nov. 7, 2008).

Conclusion

All businesses, particularly those operating in New York, should review and implement the CPB's helpful best practice recommendations to prevent -- or at least to minimize the risks and losses associated with -- data breaches and identity theft. The CPB's increased level of involvement signifies that New York is investing more resources into combating identity theft and investigating and/or helping to prosecute those New York businesses that do not do enough to protect the personal information of their customers and employees. This Guide can be used as a resource, but it is not an exhaustive review of the privacy requirements that are legally imposed on businesses in New York or in other states. In order to ensure full compliance with applicable state and federal laws, the Guide recommends speaking with a privacy professional and attorney for specific advice.

* * * * * * * * * * * * * * *

If you have any questions regarding this memorandum, please contact Francis M. Buono (202-303-1104, fbuono@willkie.com), Sophie Keefer (202-303-1142, skeefer@willkie.com), McLean Sieverding (202-303-1163, msieverding@willkie.com), Mary Underwood (202-303-1250, munderwood@willkie.com), or the attorney with whom you regularly work.

Willkie Farr & Gallagher LLP is headquartered at 787 Seventh Avenue, New York, NY 10019-6099 and has an office located at 1875 K Street, NW, Washington, DC 20006-1238. Our New York telephone number is (212) 728-8000 and our facsimile number is (212) 728-8111. Our Washington, DC telephone number is (202) 303-1000 and our facsimile number is (202) 303-2000. Our website is located at www.willkie.com.

November 26, 2008