Privacy and Data Security Update: How To Make Certain the Compliance Checklist Is Up-To-Date

ALYSA ZELTER HUTNIK AND JOHN E. VILLAFRANCO

The authors discuss the steps businesses should take to review (or re-review) their privacy and information security compliance checklists to determine whether their current information practices are up to date.

In response to new privacy and data security laws and increased enforcement by both regulators and private parties over the last several years, many businesses either have or are in the process of implementing tighter controls to protect their customers', employees', and other third parties' personal information that is stored, accessed, and shared by the business. Those measures could not come at a better time.

Alysa Zeltzer Hutnik and John E. Villafranco are attorneys with the law firm of Kelley Drye Collier Shannon in Washington, D.C. Ms. Hutnik and Mr. Villafranco specialize in counseling clients on compliance with federal and state consumer protection laws, representing clients before the Federal Trade Commission and state attorneys general in investigations concerning advertising, privacy, and data security compliance, and representing clients in private litigation concerning such practices. The authors can be reached at ahutnik@kelleydrye.com and jvillafranco@kelleydrye.com, respectively.

Published in the October 2007 Privacy & Data Security Law Journal.

FTC ACTION

The Federal Trade Commission (FTC) has made clear its intent to hold businesses responsible for lax practices that put consumers at risk of identity theft, and its 14 settlements with companies to date related to deceptive or unfair data security practices underscore that point. Nearly all of those cases subject the business to a 20-year settlement that requires the company to pay for an outside auditor to review the company's information practices biannually for 10 or 20 years and implement comprehensive data safeguards (and devote the necessary resources for full implementation in a very short period of time), and one settlement resulted in a multi-million dollar penalty.[1]

The FTC's privacy and data security enforcement efforts focus, at a minimum, on the following issues:

1. Deceptive or unsupported representations about the business's privacy or data security practices;
2. Inadequate administrative, technical, and physical safeguards of personal information;
3. Sloppy disposal practices of documents or electronic media containing personal information;
4. Providing customers with receipts that contain non-truncated credit and debit card numbers and expiration dates; and
5. The failure to provide transaction records to identity theft victims and law enforcement upon written requests.

Under Section 5 of the FTC Act, the Gramm-Leach-Bliley Act (GLBA), and the Fair Credit Reporting Act (FCRA), as amended by the Fair and Accurate Transactions Act (FACTA), depending on the violation, the FTC can seek injunctive relief, monetary redress, and/or civil penalties of up to $11,000 per violation for engaging in these practices. And given that the FTC has already provided business guidance on how to comply with all of these obligations,[2] strong FTC enforcement of violations are nearly a given.

STATE DEVELOPMENTS

Further, in addition to an FTC investigation, companies can be subject to investigations by state attorneys general who, in reaction to growing complaints over identity theft, have shown a strong interest in using state consumer protection laws to rein in unfair or deceptive business practices that put consumers' personal information at risk. For example, in 2007 alone, the Texas Attorney General has brought at least six lawsuits against companies for failing to properly dispose of documents that contain personal information in violation of Texas's disposal law.[3] Similar actions are likely to be brought throughout the country in light of the recent enactment of a number of state data security laws. Indeed, 19 states (including Texas) now specifically mandate that businesses dispose of personal information securely, 38 states and the District of Columbia mandate notice to consumers (and, depending on the state, also to regulators and credit reporting agencies) in the event of a data breach, 23 states regulate how businesses may use consumers' Social Security numbers (SSNs) and require them to protect the SSNs from public access and disclosure, and 8 states expressly require businesses to have in place administrative, technical, and physical safeguards to protect the personal information within their control. These laws — many of which allow for statutory penalties — provide state regulators with strong enforcement tools, and they are likely to be put to use in conjunction with the regulators' authority under general consumer protection laws.

CONSUMER CLASS ACTIONS

Finally, where there is regulatory interest, private litigation, particularly class action cases, are likely to follow — or, in some cases, start the trend. For example, following the enactment of state data breach notification laws, numerous class action cases were filed against many companies that incurred a data breach, including TJX companies, Pfizer, Certegy Check Services, Inc., Fidelity National Information Services, Inc., BJ's Wholesale Club, among others. Thus far, these types of cases have not been resolved favorably for the plaintiffs, mostly due to lack of proven injuries, although that result may be different in future cases given

that some of the new state laws provide for statutory damages that do not require proof of actual damages.

In addition, consumers have used the identity-theft-related provisions of FCRA as a means to challenge a business's privacy practices in court. In just the first half of this year, reports indicate that class action cases have been filed against more than 100 companies, alleging violations of Section 1681c(g) of the FCRA, 15 U.S.C. § 1681c(g).[4] That law, which provided for a right of action as of December 2006 and which the FTC also has the authority to enforce, prohibits a business from providing an electronically printed receipt containing more than the last five digits of a credit or debit card number or the expiration date. The law also allows successful plaintiffs to receive actual damages. For proven willful violations, statutory penalties ranging from $100 to $1,000 per affected consumer also may be awarded. Thus far, these cases have been brought in numerous states, including California and Pennsylvania, and have focused on businesses of all sizes.

Following this trend of cases involving businesses' use and handling of personal information, it would not be surprising to see class action cases brought against companies for violating the other identity-theft-related provisions of FCRA, including failing to provide copies of transaction records to identity theft victims and law enforcement upon written requests and in a timely manner pursuant to the statutory requirements.[5]

STEPS TO TAKE

Accordingly, it is in all businesses' interests to review (or re-review) their privacy and information security compliance checklists, and in many cases, their information practices as a whole, to determine whether their current information practices are up to date. These efforts typically include having:

- An internal or external privacy audit that identifies (1) all the channels through which personal information enters, is accessed internally, and leaves the business; (2) the risks associated with such information flow, access, and use; and (3) how to mitigate such risks, such

as reducing the collection and use of sensitive information when other less sensitive data options meet the same business objective;

- An incident response plan to follow in the event the business incurs a data breach and needs to send notice to consumers, regulators, and credit reporting agencies;
- Administrative, technical, and physical safeguards to protect the personal information within the business's control, applying these safeguards to the business's vendors that have access to and use the business's personal information, and having clear communication among the executive, legal, technical, and human resource departments of the business regarding what these obligations include and that they apply to the entire business;
- Effective data retention and disposal protocols for both hard copy and electronic media containing personal information;
- Processes in place to ensure that all electronically generated customer receipts have truncated credit or debit card information and do not contain the expiration dates;
- Protocols in place to identify a request for transaction records from an identity theft victim, properly authenticate the individual's request, and provide a timely and complete response; and
- Close and ongoing review of all privacy and data security representations to the public, whether in marketing materials, in the privacy policy, customer care scripts, press releases, or in other media, to ensure that the claims are accurate, non-misleading, and substantiated (particularly where business practices evolve over time).

While ensuring that such compliance efforts are met requires an investment of resources, taking these proactive steps now is likely to require far less than the type of resources and capital that will be necessary once forced to act in response to a regulator investigation, private litigation, public scrutiny, or all of the above.

NOTES

[1] *See, e.g., United States v. Choicepoint, Inc.*, FTC File No. 052-3069 (N.D. Ga. Dec. 6, 2006) (stipulated final judgment order), available at http://www.ftc.gov/os/caselist/choicepoint/choicepoint.shtm.

[2] *See, e.g., FTC, Info Compromise and Risk of ID Theft: Guidance for Your Business* (June 2004), available at http://www.ftc.gov/bcp/edu/pubs/business/idtheft/bus59.shtm; FTC, *Disposing of Consumer Report Information? New Rule Tells How* (June 2005), available at http://www.ftc.gov/bcp/conline/pubs/alerts/disposalalrt.shtm; FTC, *Businesses Must Provide Victims and Law Enforcement with Transaction Records Relating to Identity Theft* (May 2006), available at http://www.ftc.gov/bcp/edu/pubs/business/idtheft/bus66.shtm; FTC, *Protecting Personal Information: A Guide for Business* (Mar. 2007), available at http://www.ftc.gov/infosecurity/; FTC, *Slip Showing? Federal Law Requires All Businesses to Truncate Credit Card Information on Receipts* (May 2007), available at http://www.ftc.gov/bcp/edu/pubs/business/alerts/alt007.shtm.

[3] *See, e.g.,* Office of Texas Attorney General, *Attorney General Abbott Takes Action Against Nationwide Lender for Exposing Customer Records* (May 24, 2007), available at http://www.oag.state.tx.us/oagnews/release.php?id=2035.

[4] *See, e.g.*, Joyce E. Cutler, BNA Banking Report, *New FACTA Class Action Trend in California: Suits Over Personal Data Printed on Receipts*, V. 88, No. 11 (Mar. 19, 2007), available at http://subscript.bna.com/SAMPLES/bar.nsf/ecdc890eafc6d5bd85256b57005946be/f3b2882a769b0453852572a1001917e7?OpenDocument.

[5] A detailed analysis of how to comply with these requirements of FCRA are covered in Alysa Zeltzer Hutnik & John Villafranco, *Identity Theft: What's a Business to Do When a Consumer Calls to Complain About a Fraudulent Payment?*, Privacy and Data Security Law Journal, Vol. 1, No. 6 (May 2006).