Client Advisory

KELLEY DRYE

PRIVACY & INFORMATION SECURITY PRACTICE GROUP NOVEMBER 7, 2008

# New FTC Data Breach Settlement Involving Individual Liability and Vendor Controls; NY Releases Data Security Business Guidance

This alert provides an update on two recent data security developments:

- The alert first provides an analysis of the FTC's latest settlement with a company over a data breach. This FTC case is significant for two reasons: (1) an individual officer of the company was held liable, and (2) the business was held liable for not taking sufficient steps to confirm that *its vendor* had reasonable data security controls in place. When the vendor later incurred a breach, the FTC focused its scrutiny on the *business*, not the vendor. The case thus serves as a reminder that a business's security program should ensure that vendors with access to sensitive personal information have appropriate controls in place – both in terms of appropriate contract language, and through other reasonable due diligence, oversight, and monitoring efforts of the vendors' use of, and access to, sensitive personal data held by a business.
- The alert then summarizes a data security business guide recently released by the New York Consumer Protection Board.

## FTC SETTLES WITH MORTGAGE LENDER AND INDIVIDUAL OFFICER OVER DATA SECURITY VIOLATIONS

On November 5, 2008, a Texas-based mortgage lender, Premier Capital Lending, Inc. ("PCL") and an individual officer of the company settled with the Federal Trade Commission ("FTC") over allegations that the lender and officer violated federal data security laws – the Safeguards Rule and Privacy Rule of the Gramm-Leach-Bliley Act ("GLBA")[1] and Section 5 of the FTC Act. The FTC's complaint focused on the company's grant of access to a system containing sensitive personal information to its vendor, a third-party home seller, without taking sufficient steps to confirm that the vendor had appropriate security practices in place to protect the data. The vendor later incurred a data breach, resulting in the compromise of the lender's customers' personal information, including consumer reports. The FTC is holding the lender responsible for that third party breach.

### Relevant Facts

According to the complaint, an individual who is a co-owner of PCL (and also serves as the company's secretary and location manager) provided a third-party home seller with access to a system containing consumer reports. This access was provided so that the seller could access consumer reports from his own workplace for prospective home purchasers, and refer those individuals to PCL for home loans. In granting such access, the PCL co-owner did not assess the third-party seller's security procedures to handle, store, or dispose of personal information, or assess later on what personal information the seller maintained on its systems. The seller's computer system was later hacked and the hacker obtained access to approximately 400 consumer reports stored by the seller. Upon discovering the breach, PCL sent out written notification of the data breach to most of the affected consumers, and, a year later, after confirming that the breach covered more people, sent out notice at that point to the remaining affected consumers.

### Complaint Allegations

In its complaint, the FTC alleges that PCL failed to:

- Assess the risks in allowing its vendor (the home seller) to access consumer reports through PCL's system;

[1] 15 U.S.C. § 6801(b).

- Implement reasonable steps to address such risks, such as evaluating the vendor's computer network and taking any other steps to confirm that the vendor had appropriate data security measures in place;
- Conduct reasonable reviews of its system that allowed to the consumer reports for signs of unauthorized activity (*i.e.*, spikes of unusual increased activity or blatant irregularities); or
- Assess the full scope of consumer report information that PCL stored and made accessible, which was ultimately subject to a data security breach.

As a result of these acts and omissions, the FTC charged that PCL and its individual officer violated the GLBA Safeguards Rule, and the GLBA Privacy Rule and Section 5 of the FTC Act for misrepresentations made in its privacy policy about the extent to which PCL protected its customers' personal information.

### Consent Order Requirements

The consent order is consistent with the FTC's standard data breach settlements and requires, among other things, that PCL implement a comprehensive written information security program that conducts regular and appropriate risk assessments, is run by accountable employees, includes reasonable safeguards to control the identified security risks, and that the program includes effective controls to ensure that vendors likewise have reasonable safeguards in place. PCL also must pay a qualified data security auditor to audit the company's security program every other year for twenty (20) years and submit such reports to the FTC for review. The order did not include any monetary payments or fines.

### Case Significance

This FTC case is a reminder to businesses that regulators will attempt to hold a business responsible for its vendors' security controls (or lack thereof) if the business does not take reasonable steps to confirm that its vendors can reasonably protect personal data shared with them. Such steps typically include (1) exercising due diligence in selecting the vendors who will have access to sensitive data, (2) putting in place appropriate data security contract language in the agreement with the vendor, and (3) taking appropriate steps to confirm that vendors are compliant with such terms during the life of the agreement, particularly when red flags arise as to the vendor's handling of personal information. The risk of an officer being held personally liable for a vendor's lax security controls should make this reminder all the more stark.

## NEW YORK RELEASES DATA SECURITY BUSINESS GUIDELINES

In October 2008, the New York Consumer Protection Board published guidelines to help businesses handle and protect consumers' personal information. The "*Business Privacy Guide: How to Handle Personal Information and Limit the Prospects of Identity Theft*" (the "Guide") provides a number of recommendations for how businesses can implement and maintain a comprehensive information security program that complies with New York data security law.

Specifically, the Guide recommends that businesses:

- Identify how personal data is collected and transferred within and outside the business;
- Avoid retaining any unnecessary personal information, as well as limiting the collection and use of Social Security numbers to ensure compliance with the New York Social Security Number Protection Law;[2]
- Develop a written, comprehensive information security program to facilitate the adoption of administrative, physical, and technical safeguards for personal information;
- Limit access to personal information stored by the business;
- Secure physical and electronic access to sensitive personal information;
- Evaluate the information security practices the business's third-party service providers who will have access to personal information;

[2] New York General Business Law § 399-dd.

- Educate employees (and where relevant, customers and clients) about the business's information security practices; and
- Respond appropriately to a data breach by maintaining a response team and by becoming familiar with the data breach notification laws (and the FTC Red Flag Rules, if applicable).

These recommendations are consistent with those that the FTC and other state regulators have recommended, and would help a business achieve compliance both with New York law and many other applicable data security laws.

## KELLEY DRYE & WARREN LLP

Kelley Drye & Warren's Privacy and Information Security Practice is a leader in advising clients on privacy and information security issues and has been at the forefront of developments in this growing area of the law. Our attorneys regularly counsel clients regarding all aspects of privacy and data security compliance, including drafting and amending privacy and information security policies, advising clients on interpreting their own policies, crafting data security programs for clients, performing privacy and/or data security audits of existing business practices, drafting agreements with third parties regarding their obligations in connection with handling clients' customer data, and representing clients in connection with federal and state regulator privacy investigations regarding their privacy and data security practices.

## For more information about this Client Advisory, please contact:

**ALYSA Z. HUTNIK**
**(202) 342-8603**
**ahutnik@kelleydrye.com**

**D. REED FREEMAN**
**(202) 342-8880**
**rfreeman@kelleydrye.com**