Client Advisory

KELLEY DRYE

PRIVACY & INFORMATION SECURITY PRACTICE GROUP JANUARY 23, 2009

# FTC Files Data Security Complaint Against Mortgage Broker; Reminder Of Increased Regulatory Scrutiny Of Businesses' Data Security Practices

***Over the last three years, the Federal Trade Commission ("FTC") has settled with thirteen businesses over alleged inadequate data security practices concerning how such businesses protect consumers' personal information. The start of 2009 makes clear that the FTC intends to continue its aggressive enforcement in this area. On January 21, 2009, the FTC announced its filing of a complaint in Nevada Federal District Court against an individual mortgage broker, Gregory Navone. The complaint alleges that the defendant disposed of records containing consumers' sensitive personal information in an unsecured dumpster and failed to implement data security measures necessary for the protection of customers' sensitive personal information. The FTC also charged the defendant with misrepresenting the extent of security controls in place to protect consumer data by two of the brokerage companies owned by the defendant (First Interstate Mortgage Corporation ("FIM") and Nevada One Corporation) and the third-party service providers with which the businesses contracted.***

The case serves as a reminder of the ever-increasing scrutiny – by the FTC, State Attorneys General, and private litigants – of businesses' information security practices, and whether they are sufficiently protecting personal data against compromise and making accurate representations to the public about such security practices. This client advisory provides a summary of the key facts of the FTC's latest data security action, as well as an overview of the data security requirements applicable to most businesses.

## RELEVANT FACTS

According to the FTC, in December 2006, approximately forty boxes of the defendant's business records containing customer files were found in a publicly-available dumpster. The records consisted of tax returns, mortgage applications, bank statements, photocopies of credit cards and drivers' licenses, and credit reports. The FTC alleges that, prior to disposing of the customer records, the defendant kept them "in an insecure manner" in his garage. The FTC also alleges that the defendant falsely asserted to its customers that its mortgage businesses and their third-party service providers complied with "physical, electronic, and procedural safeguards" required by federal law.

## ALLEGATIONS

Based on these facts, the FTC charges in its complaint that the defendant failed to:

- Implement reasonable data security measures in key areas at his companies, including the physical and electronic security of sensitive consumer information and the proper collection, handling, and disposal of such information;
- Implement and monitor policies and procedures requiring the secure disposal of credit reports;
- Alert employees or third parties to such documents' sensitive nature or instruct them to take precautions;

- Ensure that employees or third parties assigned to transport documents containing sensitive personal information for disposal are qualified to do so and have received appropriate guidance or training;
- Contractually require third party service providers to maintain appropriate safeguards for customer personal information; and
- Oversee the transport of such documents for disposal or otherwise confirm that the documents are disposed of in a way that ensures that they cannot be read or reconstructed.

The FTC asserts that, as a result of these actions, the defendant violated the Fair Credit Reporting Act (FCRA) and the FCRA's Disposal Rule. In addition, the FTC asserts that the defendant violated Section 5 of the FTC Act by falsely representing the data security practices of its mortgage businesses and the practices of the businesses' third-party service providers. The FTC seeks injunctive relief and civil penalties of up to $2,500 for each separate violation.

## FEDERAL AND STATE DATA SECURITY AND DISPOSAL REQUIREMENTS

The security and disposal requirements addressed by the FTC in this latest case are substantially similar to laws enacted over the last few years by a number of states. Generally, these laws require persons and businesses handling personal information (whether of employees, customers, prospective customers, etc.) to implement and maintain a reasonable written information security program that includes applicable policies and procedures designed to protect the personal information from unauthorized access, destruction, use, modification, and disclosure.

These laws generally require persons and businesses to:

- Identify how personal data is collected and transferred within and outside the business, and identify and implement controls to protect such data at the various access points (*i.e.*, a vulnerability assessment);
- Avoid retaining personal information where there is no reasonable business justification for such retention;
- Develop a written, comprehensive information security program to facilitate the adoption of reasonable administrative, physical, and technical safeguards for personal information;
- Restrict access to personal information stored by the business, including applying additional physical and electronic access restrictions to sensitive personal information;
- Have in place applicable contract terms, and perform reasonable oversight and monitoring, regarding the information security practices of third-party service providers that has access to or handles the business's personal information (including their handling of personal data disposal, archival, data processing, and many other functions for the business);
- Train and periodically remind employees about the business's information security policies and procedures;
- Securely dispose of sensitive personal information (*i.e.*, ensure that such hard copy and electronic documents are destroyed, erased, or otherwise made unreadable prior to disposal); and
- Respond appropriately to a data breach by maintaining a response team to help ensure compliance with data breach notification laws.

Failure to have such controls in place could expose a company to legal claims by the FTC, State Attorneys General, and private litigants. Many of the applicable laws provide for injunctive relief, in which a court could require the business to implement particular security controls within an accelerated time period. These laws often also provide for statutory penalties per violation, which may be construed as per individual consumer record compromised, the number of days the company was considered not in compliance with the relevant law, or using other criteria. Accordingly, the consequences of potential enforcement action can be costly.

The increased regulatory focus on information security practices underscores more than ever that businesses would be wise to re-examine their current information security posture with involvement by key stake-holders within the company, and make appropriate adjustments

as necessary that are in line with the current legal expectations for such controls. Often, however, companies' information security programs are designed and reviewed by IT-specific personnel only, and do not involve an enterprise-wide examination and prioritization of the security controls and resources necessary to maintain and update such controls. This may result in key legal requirements left unaddressed. Given the current regulatory climate, having in place a dynamic, enterprise-wide information security program is a critical component of a risk management strategy.

## 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:

**D. REED FREEMAN**
**(202) 342-8603**
**rfreeman@kelleydrye.com**

**ALYSA Z. HUTNIK**
**(202) 342-8880**
**ahutnik@kelleydrye.com**