Privacy Client Advisory

KELLEY DRYE COLLIER SHANNON

May 16, 2006

FTC Settles Privacy Case with Nations Title Agency: Commission Alleges Failure of Title Company to Employ Reasonable Security Measures and Disposal Procedures Leading to Compromised Consumer Data.

EXECUTIVE SUMMARY

The Federal Trade Commission's ("FTC" or "Commission") 13th data security case was brought against a title company for violations of the Gramm-Leach-Bliley Act ("GLBA"), Section 5 of the FTC Act, and practices that potentially violated the Fair and Accurate Credit Transactions Act ("FACTA"). The action against Nations Title Agency, Inc., Nations Holding Company, and their president, Christopher Likens, commenced after Nations Title Agency's computer network was hacked in April 2004. Separately, ten months later, documents containing consumers' sensitive personal information were discovered in a dumpster outside Nations Holding Company offices. The settlement will require the respondents to implement a comprehensive information security program and obtain audits by an independent third party security professional every two years for twenty years.

Nations Title Agency and its subsidiary Nations Holding Company provide real estate-related services across the United States. Accordingly, the company regularly receives sensitive consumer information such as Social Security numbers, bank account numbers, and credit histories, all of which make the company a "financial institution" under the GLBA. The FTC claimed that, as a financial institution, the title company had failed to adequately secure its network, a violation of the GLBA Safeguards Rule ("Safeguards Rule"). Additionally, the discovery by a local television station of consumer documents in a dumpster likely would have been a breach of the Disposal Rule under FACTA if the discovery had occurred after the new Rule's effective date. The Commission also alleged that consumers were misled by the respondents' privacy policy, which misrepresented the level of security provided by the companies.

THE FTC CASE AGAINST NATIONS TITLE AGENCY

SAFEGUARDS RULE VIOLATION

On May 10, 2006, Nations Title Agency, Inc. ("NTA"); Nations Holding Company ("NHC"); and Christopher Likens ("Likens"), the president and sole owner of both companies, agreed to settle FTC charges that their failure to take reasonable and appropriate security measures to protect the sensitive personal information of their customers violated the Safeguards Rule.[1]

The Safeguards Rule requires companies classified as financial institutions[2] under the GLBA to protect the security, confidentiality, and integrity of consumer information by creating and maintaining a comprehensive written information security program that has reasonable administrative, technical, and physical safeguards. According to the FTC's complaint, the respondents engaged in unreasonable and inappropriate practices with respect to the sensitive consumer information in their possession. Specifically, the Commission alleged that the respondents:

- Failed to identify reasonably foreseeable internal and external risks to the security,

[1] 16 C.F.R. § 314.

[2] The GLBA broadly defines "financial institutions" to include any company that is "significantly engaged" in providing financial services or products and any company that receives sensitive information about the customers of other financial institutions.

confidentiality, and integrity of customer information both offline and online when relatively simple, low-cost defenses to common website attacks by hackers were available;

- Failed to design and implement reasonable policies and procedures concerning information safeguards in areas including employee screening and training and the collection, handling, and disposal of personal information;
- Failed to develop, implement, and maintain a comprehensive written information security program;
- Failed to investigate, evaluate, and adjust the existing information security program in light of known or identified risks and failed to regularly test and monitor the existing security program; and
- Failed to provide reasonable oversight of service providers such as third parties hired to process consumer information and assist in real estate closing and to require them by contract to implement safeguards to protect respondents' customers' information.

The FTC complaint alleged these failures allowed a computer hacker to use a common website attack to obtain unauthorized access to NTA's computer network and also resulted in improper disposal of NHC's documents in an unsecured trash dumpster.

FACTA DISPOSAL RULE

In February 2005, a television station in Kansas City discovered intact documents with sensitive personal information of consumers discarded in an unsecured dumpster that was located next to a building used by NHC. In addition to violating the Safeguards Rule, these practices would have subjected NHC to the FACTA Disposal Rule if the discovery had taken place after the Rule's effective date of June 1, 2005.[3] The FACTA Disposal Rule requires the proper disposal of information that is in consumer reports and records to prevent unauthorized access to, or use of, the information contained in those reports. Proper disposal is a flexible standard that allows the businesses and individuals responsible for the information to take appropriate steps based on the sensitivity of the information involved, the costs and benefits of the disposal methods that are available, and any relevant changes in technology.

The Commission has suggested the following policies and methods for disposing of consumer report information:

- Burn, pulverize, or shred papers containing consumer report information so that the information cannot be read or reconstructed;
- Destroy or erase electronic files or media containing consumer report information so that the information cannot be read or reconstructed; and
- Conduct due diligence and hire a document destruction contractor to dispose of material specifically identified as consumer report information consistent with the Rule. Due diligence could include:
  - Reviewing an independent audit of a disposal company's operations and/or its compliance with the Rule;

[3] 16 C.F.R. 682.

— Obtaining information about the disposal company from several references;

— Requiring that the disposal company be certified by a recognized trade association; and

— Reviewing and evaluating the disposal company's information security policies or procedures.[4]

The Commission has stated that compliance with the FACTA Disposal Rule constitutes compliance with the disposal obligations under the Safeguards Rule. The respondents did not comply with either standard.

THE PRIVACY RULE

The GLBA Privacy Rule requires that financial institutions provide consumers with a "clear and conspicuous notice that accurately reflects [its] privacy policies and practices" no later than the time when a customer relationship commences.[5] The Privacy Rule also requires the financial institution to provide this notice to the consumer annually for the length of the consumer relationship.

NTA's privacy policy claimed that the company "at all times, strives to maintain the confidentiality and integrity of the personal information in its possession and has instituted measures to guard against its unauthorized access. We maintain physical, electronic, and procedural safeguards in compliance with federal standards to protect the information."

Based on the breach and the dumpster discovery, the FTC complaint alleged that this privacy policy, which was distributed to consumers by the respondents, contained false and/or misleading statements regarding the methods used to protect consumer information. Thus, the Commission charged the respondents with a violation of the Privacy Rule and violations of Section 5 of the FTC Act.

WHAT THIS MEANS GOING FORWARD

The NTA enforcement action signals the FTC's continued commitment to investigate companies' practices that may not constitute sufficient safeguards to protect customers' personal data, including appropriate disposal of such information. Additionally, the NTA action indicates that the Commission remains dedicated to ensuring that privacy policies with regard to consumer information are not empty promises.

Perhaps the most notable aspect of this action is the FACTA Disposal Rule. Although the Disposal Rule went into effect a few months after the discovery of the documents in the dumpster, FTC Chairman Deborah Platt Majoras stated on the day of the settlement, "going forward, I think you can safely assume that tossing personal consumer report information into an unsecured dumpster runs afoul of the Disposal Rule."[6] To this end, the Consent Order specifically provides that the respondents may not violate

---

[4] FTC Business Alert: Disposing of Consumer Report Information? New Rule Tells How (June 2005) at: http://www.ftc.gov/bcp/conline/pubs/alerts/disposalalrt.htm.

[5] 16 C.F.R. §§ 313.4(a); 313.5(a)(1); § 313.6(a)(8).

[6] Remarks of Chairman Deborah Platt Majoras, Protecting Consumer Information in the 21st Century: The FTC's Principled Approach (May 10, 2006) at: http://www.ftc.gov/speeches/majoras/060510ProgressFreedomFoundationRev051006.pdf.

the FACTA Disposal Rule in the future. Although the FACTA Disposal Rule applies only to consumer reports, anyone responsible for disposing of the personal or financial information of consumers should take appropriate protective measures whenever possible. Failure to take steps to properly dispose of sensitive data may be enforced as an unfair practice under the FTC Act.

Businesses would be well-served to start (if they have not already begun) taking inventory of their business practices surrounding the collection, use, storage, and disposal of sensitive personal data (both customer and employee data) and determine whether the safeguards in place are sufficient to protect such data from unauthorized use, disclosure, and system breaches. This case demonstrates that, in addition to keeping abreast of state and federal data security pending legislation and enacted laws, businesses should be mindful that the FTC will continue to remain active in data security enforcement against all businesses that use and maintain personal data.

KELLEY DRYE COLLIER SHANNON

ADVERTISING AND MARKETING PRACTICE GROUP

Kelley Drye Collier Shannon's Advertising and Marketing practice comprises attorneys with proven success in advertising litigation and NAD proceedings; expertise in the area of advertising, promotion marketing, and privacy and data security law; and experience at the FTC, FDA, and the Offices of State Attorneys General.

We are a leader in advising clients on information privacy issues and have been at the forefront of developments in this growing area of law. Our privacy law group regularly advises clients regarding all aspects of privacy and data security law, including the Gramm-Leach-Bliley Act, the Fair Credit Reporting Act, the Health Insurance Portability and Accountability Act, the Children's Online Privacy Protection Act, the EU Data Protection Directive (as well as EU members' state laws and the Safe Harbor negotiated between the US and the EU), the FTC Act, and state privacy and data security laws.

GOVERNMENT RELATIONS AND PUBLIC POLICY PRACTICE GROUP

Our Government Relations practice helps clients interpret and shape governing laws, enabling them to maintain or achieve market leadership. Our experienced privacy attorneys work closely with our Government Relations and Public Policy practice group to stay abreast of new laws and regulations.

FOR MORE INFORMATION

For more information about this development, please contact one of our team members at (202) 342-8400 or via email:

Partners

Reed Freeman	RFreeman@KelleyDrye.com
William C. MacLeod	WMacLeod@KelleyDrye.com
Lewis Rose	LRose@KelleyDrye.com
John E.Villafranco	JVillafranco@KelleyDrye.com

Associates

Ponneh Aliabadi	PAliabadi@KelleyDrye.com
Christie Grymes	CGrymes@KelleyDrye.com
Jeffrey A. Kauffman	JKauffman@KelleyDrye.com
Jason K. Levine	JLevine@KelleyDrye.com
Gonzalo Mon	GMon@KelleyDrye.com
Dustin Painter	DPainter@KelleyDrye.com
Alysa N. Zeltzer	AZeltzer@KelleyDrye.com

Independent Contractors

Elisa A. Nemiroff	ENemiroff@KelleyDrye.com
Julie G. O'Neill	JONeill@KelleyDrye.com