

## FTC Settles With Computer Company Over Data Breach Charges

Following quickly on the heels of [our last client advisory](#) discussing recent FTC data security enforcement activity, on February 5, 2009, the FTC announced that it settled charges with Genica Corp. and Compgeeks.com (d/b/a Computer Geeks Discount Outlet and Geeks.com) over charges that the companies violated Section 5 of the FTC Act by failing to provide reasonable security to protect sensitive customer data. A detailed summary of the case is provided below, and serves as another reminder to businesses that information security (and making sure your conduct is consistent with your privacy policy) remains a key priority for regulators.

### RELEVANT FACTS

Through their sales website, for purposes of authorizing payment purchases, the companies collected sensitive personal information from consumers, including a first and last name, address, email address, telephone number, credit card number, credit card expiration date, and credit card security code. For a period of time, the companies stored that information in clear, readable text on the network on a computer that was accessible through their company website.

### COMPLAINT ALLEGATIONS

With respect to the storage of this personal information on the network, the FTC alleged that the companies engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security, including: (1) storing personal information in clear, readable text; (2) not adequately assessing the vulnerability of the companies' web application and network to commonly known or reasonably foreseeable attacks, such as "Structured Query Language" ("SQL") injection attacks; (3) not implementing simple, free or low-cost, and readily available defenses to such attacks; (4) not using readily available security measures to

monitor and control connections between computers on the network and from the network to the Internet; and (5) failing to employ reasonable measures to detect and prevent unauthorized access to personal information, such as by logging or employing an intrusion detection system.

For at least a six-month period, hackers repeatedly exploited the practices summarized above by using SQL injection attacks on the companies' website and web application. The hackers found personal information stored on the network and exported the information of hundreds of customers, including credit card numbers, expiration dates, and security codes, over the Internet to outside computers.

In the companies' privacy policy, they represented that they implemented reasonable and appropriate measures to protect personal information against unauthorized access: *i.e.*, "We use secure technology, privacy protection controls, and restrictions on employee access in order to safeguard your information." The FTC concluded that the safeguards implemented were not sufficient, and thus, the companies' safeguard representations were allegedly false or misleading information, which the FTC charged was a violation of Section 5 of the FTC Act.

### CONSENT ORDER REQUIREMENTS

The Companies settled the charges with the FTC. The terms of the settlement are consistent with other FTC data breach settlements. Specifically, the Order:

- bars the companies from making deceptive privacy and data security claims;
- requires them to implement and maintain a comprehensive information-security program that includes administrative, technical, and physical safeguards;
- requires the companies to obtain, every other year for 10 years, an audit from a qualified, independent, third-

party professional to ensure that the security program meets the standards of the order; and

- contains standard record-keeping provisions to allow the FTC to monitor compliance.

### **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) 342-8880  
[rfreeman@kelleydrye.com](mailto:rfreeman@kelleydrye.com)

**ALYSA Z. HUTNIK**  
(202) 342-8603  
[ahutnik@kelleydrye.com](mailto:ahutnik@kelleydrye.com)