Analysis of Proposed Consent Order to Aid Public Comment
In the Matter of Genica Corporation and Compgeeks.com, File No. 082-3113

The Federal Trade Commission has accepted, subject to final approval, a consent agreement from Genica Corporation ("Genica") and Compgeeks.com, also doing business as Computer Geeks Discount Outlet and Geeks.com ("Compgeeks.com").

The proposed consent order has been placed on the public record for thirty (30) days for receipt of comments by interested persons. Comments received during this period will become part of the public record. After thirty (30) days, the Commission will again review the agreement and the comments received, and will decide whether it should withdraw from the agreement and take appropriate action or make final the agreement's proposed order.

Genica and its wholly-owned subsidiary, Compgeeks.com, (collectively "respondents") sell computer systems, peripherals, and consumer electronics to consumers over the internet, including through a website (www.geeks.com) operated by Compgeeks.com. Respondents operate a computer network that consumers use, in conjunction with the www.geeks.com website and web application, to obtain information and to buy their products. In selling products through the www.geeks.com website, respondents routinely collect sensitive information from consumers to obtain authorization for credit card purchases, including a first and last name, address, e-mail address, telephone number, credit card number, credit card expiration date, and credit card security code (hereinafter "personal information"). This information is particularly sensitive, because it can be used to facilitate payment card fraud and other consumer harm. This matter concerns alleged false or misleading representations respondents made about the security they provided for this information.

The Commission's complaint alleges that respondents represented that they implemented reasonable and appropriate security measures to protect the privacy and confidentiality of personal information. The complaint alleges that this representation was false because respondents engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security for sensitive personal information stored on their network. Among other things, respondents allegedly: (1) stored personal information in clear, readable text; (2) did not adequately assess the vulnerability of their web application and network to commonly known or reasonably foreseeable attacks, such as "Structured Query Language" ("SQL") injection attacks; (3) did not implement simple, free or low-cost, and readily available defenses to such attacks; (4) did not use readily available security measures to monitor and control connections between computers on the network and from the network to the internet; and (5) failed to employ reasonable measures to detect and prevent unauthorized access to personal information, such as by logging or employing an intrusion detection system.

The complaint further alleges that since at least January 2007 and continuing through at least June 2007, hackers repeatedly exploited these vulnerabilities by using SQL injection attacks on the www.geeks.com website and web application. Through these attacks, the hackers allegedly found personal information stored on respondents' network and exported the

information of hundreds of customers, including credit card numbers, expiration dates, and security codes, over the internet to outside computers.

The proposed order applies to personal information respondents collect from or about consumers. It contains provisions designed to prevent respondents from engaging in the future in practices similar to those alleged in the complaint.

Part I of the proposed order prohibits respondents, in connection with the advertising, marketing, promotion, offering for sale, or sale of any product or service, from misrepresenting the extent to which respondents maintain and protect the privacy, confidentiality, or integrity of any personal information collected from or about consumers.

Part II of the proposed order requires respondents to establish and maintain a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers. The written security program must contain administrative, technical, and physical safeguards appropriate to respondents' size and complexity, the nature and scope of respondents' activities, and the sensitivity of the personal information collected from or about consumers. Specifically the order requires respondents to:

- Designate an employee or employees to coordinate and be accountable for the information security program;

- Identify material internal and external risks to the security, confidentiality, and integrity of personal information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks;

- Design and implement reasonable safeguards to control the risks identified through risk assessment, and regularly test or monitor the effectiveness of the safeguards' key controls, systems, and procedures;

- Develop and use reasonable steps to retain service providers capable of appropriately safeguarding personal information they receive from respondents and requiring service providers by contract to implement and maintain appropriate safeguards; and

- Evaluate and adjust respondents' information security program in light of the results of the testing and monitoring, any material changes to respondents' operations or business arrangements, or any other circumstances that respondents know or have reason to know may have a material impact on the effectiveness of their information security program.

Part III of the proposed order requires that respondents, in connection with the online advertising, marketing, promotion, offering for sale, or sale of any product or service to consumers, obtain within 180 days, and on a biennial bases thereafter for a period of ten (10) years, an assessment and report from a qualified, objective, independent third-party professional, certifying, among other things, that respondents have in place a security program that provides protections that meet or exceed the protections required by Part II of the proposed order; and (2) respondents' security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of consumers' personal information is protected.

Parts IV through VIII of the proposed order are reporting and compliance provisions. Part IV requires respondents to retain documents relating to their compliance with the order. For most records, the order requires that the documents be retained for a five-year period. For the third-party assessments and supporting documents, respondents must retain the documents for a period of three years after the date that each assessment is prepared. Part V requires dissemination of the order now and in the future to persons with responsibilities relating to the subject matter of the order. Part VI ensures notification to the FTC of changes in corporate status. Part VII mandates that respondents submit an initial compliance report to the FTC, and make available to the FTC subsequent reports. Part VIII is a provision "sunsetting" the order after twenty (20) years, with certain exceptions.

The purpose of the analysis is to aid public comment on the proposed order. It is not intended to constitute an official interpretation of the proposed order or to modify its terms in any way.