

**\$275,000 FINE FOR FAILURE TO USE
ADEQUATE SECURITY MEASURES**

by Francoise Gilbert, CIPP*
IT Law Group – Palo Alto, CA

The Security & Exchange Commission has fined a broker-dealer \$275,000 for failure to use adequate security measures to protect customer information.

In its settlement with the SEC, (available at <http://www.sec.gov/litigation/admin/2008/34-58515.pdf>) the company has agreed to devise and implement a policy and a set of procedures for training its employees and independent contractors with respect to the protection of customer records and information. In addition, it will engage an independent auditor to review its privacy and security procedures and will implement the recommendation of this independent party in order to comply with the applicable Safeguards Rule within 180 days of the issuance of the SEC Order.

* * * * *

It is not just the Federal Trade Commission who is monitoring the data protection practices of companies. On September 11, 2008, the SEC and LPL Financial Corporation (LPL) settled an administrative and cease-and-desist order for LPL's violations of the Securities Exchange Act of 1934 (Sections 15(b) and 21C) and the Investment Advisers Act of 1940 (Sections 203(e) and 203(k)).

LPL, registered with the Commission as a broker-dealer, investment adviser, and transfer agent, is subject to the Safeguards Rule of Regulation S-P (17 CFR Section 248.30(a)). The Safeguards Rule requires broker-dealers to adopt appropriate written policies and procedures designed to protect customer information.

These policies and procedures must be reasonably designed to:

- ensure the security and confidentiality of customer records and information;
- protect against any anticipated threats or hazards to the security or integrity of customer records and information; and

- protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to a customer.

Security Incidents: According to the SEC, BranchNet, LPL's online trading platform for its independent contractor registered representatives (RRs), failed to implement the adequate security measures. LPL did not implement increased security measures and adopt policies and procedures reasonably designed to protect customer information, despite it having known of the vulnerabilities of its branch offices since 2006 and having suffered unauthorized access to its computer systems between July 2007 and February 2008. The security breach incidents resulted in the unauthorized access of the non-public information of at least 10,000 customers: thirteen online accounts of LPL RRs were accessed and 209 unauthorized trades were placed, a total of about \$700,000 in unauthorized trades and securities of nineteen different companies were placed. LPL was able to block most of the unauthorized trade requests. It reversed trade requests that were executed and compensated customers for trading losses due to the incident, which totaled approximately \$98,900.

Poor Security Measures Identified: In between July and September 2006, LPL conducted an internal audit. The audit revealed several deficiencies in the BranchNet system, including: the system allowed for the use of weak passwords; passwords were not set to expire after certain period of time; users could not change their own passwords; there was no automatic lockout feature due to unsuccessful login attempts; and the automatic session timeout was set at eight hours. The audit also revealed that over 300 LPL IT employees had access to a list of passwords and a number of former employees likely had access to the same list before leaving the firm. The results of the audit were submitted to LPL's senior management members and executive risk committee in which they were warned of the vulnerabilities of the BranchNet system. Despite the warnings, LPL failed to take immediate action.

Insufficient Policies: The SEC found that LPL failed to have a customer information policy for its employees or branch RRs describing its overall program designed to protect customer information. LPL's existing policies were not reasonably designed to protect customer information: they were incomplete and insufficient with regards to addressing administrative, technical, physical safeguards to protect customer information at the branch offices. Materials distributed to the branch offices were often suggestions or recommendations and not mandates on safeguarding customer information. Before mid-2006, LPL failed to reasonably evaluate the security controls of BranchNet, despite having had outside IT consultants to conduct vulnerability checks.

Fine and Requirements: Under the agreement with the SEC, LPL will train its employees on security issues. It must also hire an independent consultant and must adopt all recommendations made by the independent consultant within 180 days after the Order. In addition to the requirements above, LPL must pay the Securities and Exchange Commission a civil penalty of \$275,000.

Assessment: This recent SEC Order is a reminder that institutions regulated by the Security & Exchange Commission – *as well as many other organizations subject to similar regimes under different laws* – are required to implement substantial privacy and security measures in order to protect the personal information entrusted to them. Even when the applicable regulation does not provide specific or detailed instructions on the types of information security or privacy measures required – as was the case for Regulation S-P – companies must ensure that they follow the current best practices and standards.

Companies may wish to review their compliance program and determine whether it meets the current data protection standards and take at least the following steps – even if some measures might already be in place:

- **Identify the systems and information that need to be protected**

- **Conduct an assessment of the risks to which these systems and information may be exposed**
- **Develop (or update) and implement security measures designed to manage and control the specific risks identified**
- **If measures are already in place, ensure that the program is properly implemented and effective; and revise the program as necessary to take into account ongoing changes**
- **Review third party service provider arrangements**
- **Implement security awareness training and education**

* Copyright 2008, Françoise Gilbert, IT Law Group, Palo Alto, CA. www.itlawgroup.com All rights reserved.

Françoise Gilbert is an attorney and a Certified Information Privacy Professional (CIPP). She is the Managing Director of IT Law Group, www.itlawgroup.com, a law firm based in Palo Alto, California, with offices in Paris, France. She focuses on information privacy and security, and data governance.

Ms. Gilbert is listed in the 2008 edition of "The Best Lawyers in America", Chambers USA, and Who's Who in E-Commerce. She holds a graduate degree in Mathematics from Paris University (France) and law degrees from Paris University (France) and Loyola University in Chicago. She is admitted to practice law in California, Illinois, and France.

Contact Information:

Email: fgilbert@itlawgroup.com Phone: (1) 650-804-1235.