



Tracker impact analysis: SEC fines LPL Financial Corporation for regulation S-P violations

Nov 06 2008 [Morgan Lewis & Bockius LLP](#)

The Securities and Exchange Commission recently settled an enforcement matter with LPL Financial Corporation ("LPL" or "the Firm"), alleging that LPL violated regulation S-P in connection with safeguarding its clients' nonpublic personal information. The Commission alleged that LPL failed to evaluate adequately the security of an on-line trading platform used by the Firm's brokers to place trades for clients, and despite being aware that an internal audit suggested its measures for safeguarding customer information needed to be enhanced, it failed to implement policies and procedures reasonably designed to protect its clients' nonpublic personal information. As part of the settlement, LPL consented to pay a \$275,000 civil money penalty and to retain an independent consultant to review its regulation S-P protocols.

As discussed below, the *LPL* action is significant because it reflects the first time that the Commission brought an enforcement matter under regulation S-P, let alone one with a six-figure penalty, against a firm for failing to protect adequately against unauthorized access to clients' nonpublic personal information.

Main issues arising

Regulation S-P and the Commission's prior actions to enforce it

The safeguards rule of regulation S-P requires broker/dealers, investment companies and registered investment advisers to adopt policies and procedures reasonably designed to guard the security of their clients' nonpublic personal information, protect against anticipated threats to the security of such information, and prevent unauthorized access to and use of clients' nonpublic personal information that could result in significant harm or inconvenience to clients. Firms are required to provide their clients with notice of these policies and procedures.

Although the Commission previously brought cases relating to brokerage account intrusion and misappropriation of client-identifying information, prior to the *LPL* matter, the SEC had not brought charges under regulation S-P against the firm that was the victim's financial service provider.

SEC enforcement actions in prior cases involving account intrusions, as well as criminal cases brought by the Department of Justice, targeted the intruders. For example, in late 2006 and early 2007, the Commission filed suits in federal district court against hackers from Estonia and India who used stolen usernames and passwords to commit securities fraud. In some instances, the perpetrators first purchased thinly traded microcap securities. Then they hacked into on-line brokerage accounts and purchased shares of the same microcap securities in order to drive up the trading price before selling the microcap positions in their own accounts at a substantial profit. We understand anecdotally that in at least some of these cases, the firms cooperated with the regulators and made clients whole for losses, which may have been factors in the Commission's decision not to charge the firms with violations of regulation S-P.

The Commission also brought a case involving regulation S-P against a broker for misappropriating from his employer client-identifying information for personal gain. In the matter of *Sidney Mondschein* involved allegations by the Commission that between December 2002 and August 2005, Sidney Mondschein, a registered representative, illegally profited by sharing confidential personal information of more than 500 of his firm's brokerage clients. Mondschein sold this confidential information as sales "leads" to enable insurance agents to solicit these clients. In return, many of the insurance agents recommended Mondschein to their clients. According to the settlement release, Mondschein's conduct aided and abetted his broker/dealer's violation of regulation S-P, although his employer does not appear to have been charged to date in this matter. Pursuant to the settlement, Mondschein was barred from association with any broker or dealer for five years.

The only regulation S-P case that the Commission brought against a broker/dealer prior to the *LPL* matter was *in the matter of NEXT Financial Group, Inc.*, which involved very different facts from the account intrusion and *Mondschein* cases. The Commission alleged that NEXT Financial Group, Inc. ("NEXT") violated regulation S-P by permitting registered representatives who were leaving the firm to take clients' personal financial information with them and aided and abetted other firms' violations of regulation S-P by encouraging and assisting newly recruited registered representatives to bring nonpublic personal information about their former firms' clients to NEXT. In 2008, an administrative law judge issued an initial decision that imposed a \$125,000 fine on NEXT.

The *NEXT* case involved *intentional* conduct and policies approved by the respondent firm, in contrast to the internal misappropriation of client-identifying data by an employee in *Mondschein* or unauthorized account intrusions by outsiders in the actions against hackers. Until *LPL*, the Commission had not charged a broker/dealer for failing to safeguard clients' nonpublic personal data from unauthorized account intrusion or misappropriation.

In the matter of LPL

LPL did not provide on-line trading capability directly to clients. Rather, LPL allowed its registered representatives to place client trades, open new accounts, and review detailed account and commission information using BranchNet, the firm's proprietary trading platform. Between July 2007 and February 2008, unauthorized individuals attempted to place \$700,000 in trades in 68 LPL client accounts using misappropriated BranchNet broker login information. While LPL successfully detected and blocked most of the unauthorized trade requests, in a few instances the trades were executed, resulting in approximately \$98,900 in losses to LPL's clients. LPL promptly compensated its clients for their losses.

LPL consented to findings that its conduct violated the safeguards rule of regulation S-P because it did not have written policies reasonably designed to safeguard customer records and information and failed to evaluate security controls for its on-line trading platform. To settle the matter, the Firm agreed to pay a civil money penalty of \$275,000, devise and implement new policies and procedures for training personnel on the protection of client information, and retain an independent consultant to review and make recommendations concerning LPL's policies and procedures with respect to the safeguarding provisions of regulation S-P.

Compliance lessons learned from the LPL matter

The fact that the Commission brought a case against LPL and insisted upon a civil money penalty and the retention of an independent consultant highlights two important compliance takeaways: (1) the need for firms to act promptly to address operational or other inadequacies upon their discovery; and (2) the increasing regulatory focus on regulation S-P.

A critical component of the *LPL* settlement appears to be the Commission's perception that LPL failed to respond adequately to weaknesses in its regulation S-P safeguards promptly after it became aware of them. Almost one year before the account intrusions at issue occurred, LPL had conducted an internal audit of BranchNet's security controls. The audit report revealed to senior management weaknesses concerning BranchNet broker passwords, including that the passwords were not sufficiently long or complex and did not expire after a specified period of time. These perceived deficiencies increased the likelihood that a hacker could obtain confidential information and conduct unauthorized trades. Yet, according to the Commission, when the security breaches began in July 2007, LPL had not yet taken steps to improve its privacy policies and procedures in response to the internal audit.

The notion that the Commission will not tolerate what it perceives to be slow response time to known deficiencies is not a new theme. For example, an SEC release announcing the settlement of an administrative proceeding against Morgan Stanley last year emphasized that the firm had been made aware of deficiencies and inaccuracies with regard to its trade confirmations four years before it undertook an official internal review of the issue at the Commission's urging. Morgan Stanley consented to paying a fine of \$7,500,000 to settle the matter. As with the *Morgan Stanley* case, the *LPL* matter serves as a reminder that firms must respond swiftly upon discovery of compliance breaches.

Second, the regulatory focus on regulation S-P cases has been, and likely will continue to be, on the upswing. Both FINRA and the SEC named protection of customer information among their top examination priorities for 2008. Earlier this year, the Commission proposed amendments to strengthen regulation S-P after observing "a significant increase in information security breaches" involving SEC-regulated entities, particularly with respect to on-line brokerage account intrusions. The proposed rule release expressed concern that "some firms do not regularly reevaluate and update their safeguarding programs to deal with these increasingly sophisticated methods of attack." These amendments, among other provisions, contain more detailed standards for implementing information security programs and responding to security breaches, including:

- identifying in writing the employee(s) charged with coordinating the firm's information security program;
- identifying reasonably foreseeable security risks that could jeopardize security of clients' nonpublic personal information and implementing related safeguards to defend against such risks;
- testing and monitoring of the firm's information security program;
- training employees concerning the information security program; and
- overseeing service providers that have access to the nonpublic personal information of firm clients.

The amendments also would result in an amended regulation S-P that conforms more closely to privacy regulations implemented by federal banking agencies and the Federal Trade Commission.

In light of this increased focus on regulation S-P, firms should pay careful attention to their regulation S-P compliance and not rely on "off-the-shelf" privacy policies and procedures. Firms also should make sure that their written policies and procedures are tailored to detect and prevent violations of regulation S-P in light of their particular business models. Finally, firms should disseminate their policies to employees and provide adequate training.

For more than a century, Morgan Lewis lawyers have helped clients achieve their business goals and clients have come to rely on the firm for its tradition of professional excellence, integrity and client service. Morgan Lewis is consistently ranked among the world's leading law firms because we deliver effective solutions to our clients. With over 1,300 lawyers and 300 other professionals (including technical specialists, patent agents and paralegals) in 22 offices worldwide, Morgan Lewis offers a complete range of practices and are well positioned to meet clients' critical legal needs. From day-to-day business decisions to the most complex and global business transactions, our clients rely on the firm to guide them through all of their legal needs.

This article was written by Michael S Kraut and Ben A Indek, partners in Morgan Lewis' litigation practice.

Namita E Mani, an associate at Morgan Lewis also contributed to this article.

Related content

Related Articles

- ▶ [25 Sep 2008 - Cyber fraud artists get more sophisticated, more international](#)
- ▶ [19 Jun 2008 - NEXT Financial gets mixed win over alleged privacy violations](#)

News by Subject

- ▶ [Data protection and privacy](#)
- ▶ [Systems and controls](#)
- ▶ [Client Assets](#)
- ▶ [Compliance Monitoring and Oversight](#)
- ▶ [Sanctions, Regulatory Enforcement and Criminal Proceedings](#)

Directory

- ▶ [Federal Trade Commission - USA](#)
- ▶ [Securities and Exchange Commission \(USA\)](#)
- ▶ [FINRA: Financial Industry Regulatory Authority](#)

News by Country

- ▶ [United States](#)

Related Rulebooks

SEC Rules (17 CFR Ch. II)

- ▶ [Part 248 Regulation S-P: Privacy of consumer financial information](#)

Securities and Exchange Commission Materials

- ▶ [2008-193 SEC Charges LPL Financial for Failing to Protect Customer Privacy \(September 11, 2008\)](#)

Complinet | Connected Compliance TM

© 2008 Complinet Ltd and its contributors. All rights reserved.

[Terms & Conditions](#)

[Privacy statement](#)

[Accessibility](#)

[RSS](#)

[Contact Us](#)

[Disclaimer](#)