



PRIVACY, DATA SECURITY & INFORMATION LAW UPDATE

The Privacy, Data Security & Information Law Practice of Sidley Austin LLP

We offer clients an inter-disciplinary, international group of lawyers focusing on the complex national and international issues of data protection and cyber law. The group includes regulatory compliance lawyers, litigators, financial institution practitioners, healthcare lawyers, EU specialists, IT licensing and marketing counsel, intellectual property, and white collar lawyers. Sidley provides services in the following areas:

Privacy and Internet Litigation and Regulatory Advice
Data Breach, Incident Response, and Cybercrime Advice
Global Data Protection and Information Security
International Data Transfer Solutions
Outsourcing and Cross-Border Issues
Gramm-Leach-Bliley and Financial Privacy
HIPAA and Healthcare Privacy
Workplace Privacy and Employee Monitoring
Cyberlaw, E-Commerce, and Internet Issues
Unfair Competition and Consumer Protection
Trademark and Copyright Litigation and Counseling
Website Policies and Domain Name Protection
Records Retention and Electronic Discovery

To receive future copies of Practice Update via email, please send your name, company or firm name and email address to Rachel Shields at rshields@sidley.com.

Attorney Advertising - For purposes of compliance with New York State Bar rules, our headquarters are Sidley Austin LLP, 787 Seventh Avenue, New York, NY 10019, 212.839.5300 and One South Dearborn, Chicago, IL 60603, 312.853.7000. Prior results do not guarantee a similar outcome.

SEC Enforcement Action for Lax Information Security After Data Breach Involving Independent Registered Representatives

The Securities and Exchange Commission (SEC) has issued another indication that they are serious about information security. On September 29, the SEC issued an order instituting administrative and cease and desist proceedings against Commonwealth Financial Network for its failure to protect customer data as required by Rule 30(a) of Regulation S-P, better known as the SEC's Safeguards Rule under the Gramm-Leach-Bliley Act. The Safeguards Rule requires covered institutions (brokers, dealers and investment companies, and registered investment advisors) to adopt written policies that protect the confidentiality of customer data, guard against threats to the security of the data, and protect against unauthorized access to the records that could result in harm to the customer. By failing to require its independent registered representatives to deploy antivirus software, and to follow up on indications that a representative had a virus that could compromise its information security, the SEC believes that Commonwealth Financial Network failed to comply with the Rule. As a result, the SEC ordered the firm to cease and desist from committing these and any future Safeguard Rule violations, be censured for its failures, and pay a penalty of \$100,000.

Commonwealth's Failure to Require Information Security

Commonwealth has a decentralized advisor structure with independent contractor registered representatives operating out of over 1,000 branch offices. These representatives access the commonwealth's intranet and online trading platform from their own computers and software. Commonwealth provides IT services to troubleshoot technical problems, and had written information security policies on its intranet that required its representatives to maintain the security of their customer information. Significantly, Commonwealth only *recommended* antivirus software, but did not require it.

This **Sidley Update** has been prepared by Sidley Austin LLP for informational purposes only and does not constitute legal advice. This information is not intended to create, and receipt of it does not constitute, a lawyer-client relationship. Readers should not act upon this without seeking advice from professional advisers.

According to the SEC's Order, in September 2008, one of Commonwealth's representatives called the help desk about a potential software virus. The IT desk recommended the representative get antivirus software, and did not follow up regarding the incident. The representative called again in November 2008, and the IT desk noted the computer had "a major virus" and recommended the representative have his computer repaired locally. The representative followed this advice, but it was too late. A hacker had obtained the representative's login credentials through a keystroke/keylogger virus, and was able to log on, search the system for accounts with cash balances, and obtain personal data for 368 accounts—including the account name, number, registration type, net worth, cash balance and the last 4 digits of the owner's Social Security number. The hacker then placed 18 stock purchase orders, amounting to over \$500,000 in unauthorized purchases within ten minutes of trading. Commonwealth's clearing broker-dealer detected the activity and blocked the trading. Commonwealth took responsibility for the purchases, canceled them and absorbed the loss. It also notified the 368 account holders of the breach of their personal information, and reported the incident to the SEC.

The SEC found that Commonwealth's failure to *require* basic information security such as antivirus software, failing to follow up after becoming aware that a virus might threaten the integrity of its system, and generally failing to have procedures in place to review its representatives' security measures or audit their computers was not reasonable or adequate compliance with the Safeguard Rule.

Pending Amendments Will Enhance Information Security Requirements

This enforcement action comports with the SEC's pending March 2008 proposal to revise Regulation S-P to strengthen information security requirements—including a mandatory breach notification procedure. While the proposal has not been finalized, this enforcement action certainly can be seen as an indication that the SEC is interested in a more active role in

information security, and protecting consumers from identity theft. In explaining the proposed revision of Regulation S-P, the SEC¹ stated:

- In the last two years, we have seen a significant increase in information security breaches involving institutions we regulate. Perhaps most disturbing is the increase in incidents involving the takeover of online brokerage accounts. The financial services sector also is a popular target for online targeted attacks....
- Many firms in the securities industry are aware of these problems and have appropriate safeguards in place to address them. We are concerned, however, that some firms do not regularly reevaluate and update their safeguarding programs to deal with these increasingly sophisticated methods of attack.

While the specific standards of the final rule have not yet been released, the recent enforcement action suggests that controlling information security of independent registered representatives is the responsibility of the parent broker-dealer and that requiring antivirus software, conducting regular security audits of computer systems, and taking proactive response to indications of potential system compromise would be minimum requirements.

The SEC's strategic plan² posted on the SEC website in October 2009 further highlights consumer information security. The strategic plan states, "[t]he SEC intends to consider enhancing the information that a broker-dealer underwriting a primary offering of municipal securities must

¹ SEC Proposed Rule Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Personal Information, 73 Fed. Reg. 50, 13693 (March 13, 2008), available at <http://www.sec.gov/rules/proposed/2008/34-57427fr.pdf>.

² SEC, Draft Strategic Plan for Fiscal Years 2010-2015, 35, available at <http://www.sec.gov/about/secstratplan1015.pdf> (emphasis added).

determine that an issuer will provide to shareholders, as well as to improve protections against identity theft and investor understanding of financial privacy notices. . . .”

We recommend covered institutions reevaluate their information security practices and update their written policies to limit risk of liability under Regulation S-P—as well as the financial and reputational expense that can come from a breach of security.

If you have questions about the contents of this update, please contact one of the attorneys listed below, or the Sidley attorney with whom you regularly work:

Alan Charles Raul
+1.202.736.8477
araul@sidley.com

Edward McNicholas
+1.202.736.8010
emcnicholas@sidley.com

Karl F. Kaufmann
+ 1.202.736.8133
kkaufmann@sidley.com

Michael F. McEneny
+1.202.736.8368
mmceneny@sidley.com

BEIJING BRUSSELS CHICAGO DALLAS FRANKFURT GENEVA HONG KONG LONDON LOS ANGELES NEW YORK SAN FRANCISCO SHANGHAI SINGAPORE SYDNEY TOKYO WASHINGTON, D.C.

www.sidley.com

Sidley Austin LLP, a Delaware limited liability partnership which operates at the firm's offices other than Chicago, London, Hong Kong, Singapore and Sydney, is affiliated with other partnerships, including Sidley Austin LLP, an Illinois limited liability partnership (Chicago); Sidley Austin LLP, a separate Delaware limited liability partnership (London); Sidley Austin LLP, a separate Delaware limited liability partnership (Singapore); Sidley Austin, a New York general partnership (Hong Kong); Sidley Austin, a Delaware general partnership of registered foreign lawyers restricted to practicing foreign law (Sydney); and Sidley Austin Nishikawa Foreign Law Joint Enterprise (Tokyo). The affiliated partnerships are referred to herein collectively as Sidley Austin, Sidley, or the firm.

SIDLEY AUSTIN LLP
SIDLEY