UNITED STATES OF AMERICA
Before the
SECURITIES AND EXCHANGE COMMISSION

SECURITIES EXCHANGE ACT OF 1934
Release No. 60733 / September 29, 2009

INVESTMENT ADVISERS ACT OF 1940
Release No. 2929 / September 29, 2009

ADMINISTRATIVE PROCEEDING
File No. 3-13631

In the Matter of **Commonwealth Equity Services, LLP d/b/a Commonwealth Financial Network,** **Respondent.**	ORDER INSTITUTING ADMINISTRATIVE AND CEASE-AND-DESIST PROCEEDINGS PURSUANT TO SECTIONS 15(b) AND 21C OF THE SECURITIES EXCHANGE ACT OF 1934, AND SECTIONS 203(e) AND 203(k) OF THE INVESTMENT ADVISERS ACT OF 1940, MAKING FINDINGS, AND IMPOSING REMEDIAL SANCTIONS AND A CEASE-AND-DESIST ORDER

I.

The Securities and Exchange Commission ("Commission") deems it appropriate and in the public interest that public administrative and cease-and-desist proceedings be, and hereby are, instituted pursuant to Sections 15(b) and 21C of the Securities Exchange Act of 1934 ("Exchange Act"), and Sections 203(e) and 203(k) of the Investment Advisers Act of 1940 ("Advisers Act") against Commonwealth Equity Services, LLP d/b/a Commonwealth Financial Network ("Commonwealth" or "Respondent").

II.

In anticipation of the institution of these proceedings, Respondent has submitted an Offer of Settlement (the "Offer") which the Commission has determined to accept. Solely for the purpose of these proceedings and any other proceedings brought by or on behalf of the Commission, or to which the Commission is a party, and without admitting or denying the findings herein, except as to the Commission's jurisdiction over it and the subject matter of these proceedings, which are admitted, Respondent consents to the entry of this Order Instituting

Administrative and Cease-and-Desist Proceedings Pursuant to Sections 15(b) and 21C of the Securities Exchange Act of 1934, and Sections 203(e) and 203(k) of the Investment Advisers Act of 1940, Making Findings, and Imposing Remedial Sanctions and a Cease-and-Desist Order ("Order"), as set forth below.

III.

On the basis of this Order and Respondent's Offer, the Commission finds[1] that

Summary

1. These proceedings arise out of the violations by Commonwealth, a registered broker-dealer and investment adviser, of Rule 30(a) of Regulation S-P (17 C.F.R. § 248.30(a)) (the "Safeguards Rule"), which requires broker-dealers and Commission-registered investment advisers to adopt written policies and procedures reasonably designed to protect customer information. At all relevant times, Commonwealth recommended – but did not require – that its registered representatives maintain antivirus software on their computers, which the registered representatives used to access customer account information on the firm's intranet and trading platform. As a result, Commonwealth's customer information was left vulnerable to unauthorized access. In addition, Commonwealth did not have procedures in place to adequately review its registered representatives' computer security measures. In particular, Commonwealth's internal auditors did not audit branch office computers to determine whether antivirus software was installed, nor did Commonwealth have procedures in place to follow up on potential computer security issues uncovered during branch audits or when registered representatives contacted Commonwealth's information technology help desk for computer-related assistance.

2. In November 2008, an unauthorized party ("intruder") obtained the login credentials of a Commonwealth registered representative through the use of a computer virus and was thereby able to access Commonwealth's intranet. The intruder accessed a list of 368 of the representative's Commonwealth customer accounts (which included certain customer account information) and entered unauthorized purchase orders in eight of those accounts before the activity was detected by Commonwealth's clearing broker-dealer and the intruders were blocked from further trading.[2] Although Commonwealth absorbed the monetary losses, its failures allowed the intruder to have access to certain customer information relating to 368 of the representative's customer accounts.

[1] The findings herein are made pursuant to Respondent's Offer of Settlement and are not binding on any other person or entity in this or any other proceeding.

[2] The 368 accounts that were improperly accessed included both broker-dealer customer accounts and investment advisory client accounts. For convenience, unless otherwise specified, this Order refers to all of Commonwealth's accounts, including the 368 accounts as customer accounts.

Respondent

3. Commonwealth, headquartered in Waltham, Massachusetts, is registered with the Commission as a broker-dealer (File No. 8-24040) and investment adviser (File No. 801-41541). Commonwealth is privately owned, employs approximately 400 people at its main office in Waltham and has an additional operational office in San Diego, California that employs approximately 55 people and also serves as an Office of Supervisory Jurisdiction ("OSJ"). Commonwealth has approximately 1,600 independent contractor registered representatives ("registered representatives") operating from approximately 1,069 branch offices, 110 of which are designated as OSJs. Commonwealth also has approximately 19 unregistered, non-branch locations. Commonwealth offers a variety of products and services, including general securities, mutual funds, and variable insurance products to its retail customer base. Commonwealth has over 165,000 customer brokerage accounts and approximately 95,000 investment advisory client accounts. It conducts approximately 200,000 trades per month in these accounts.

Background

4. At all relevant times, Commonwealth did not directly provide its customers with an online trading platform. Rather, Commonwealth provided its registered representatives with access to its clearing broker's proprietary trading platform through Commonwealth's intranet trading site. Using login credentials, Commonwealth's registered representatives could access the trading platform online from any computer with an Internet connection. Pursuant to its independent contractor model, Commonwealth required its branch office registered representatives to supply their own computer hardware and software.

5. In or around November 2008, an unauthorized party obtained the login credentials of one of Commonwealth's registered representatives through the use of a malware/keystroke logger virus. The virus was placed on the registered representative's computer, which at the time did not have antivirus software properly employed. In early November 2008, the intruder, using the registered representative's login credentials, entered Commonwealth's intranet site and viewed information on how to execute trades. Approximately a week later, the intruder used the same registered representative's login credentials to enter the trading platform. The intruder ran a search query for the Commonwealth registered representative's customer accounts with cash balances in excess of a certain amount, generating a list of 368 accounts. By doing so, the intruder had access to the account name, account number, account registration type, account net worth, cash balance, and the last four digits of the account owner's Social Security number for all 368 accounts.

6. On that same day, the intruder placed or attempted to place eighteen unauthorized purchase orders for the common stock of one publicly-traded company in eight of the 368 customer accounts identified, totaling over $523,000 of unauthorized purchases. Within ten minutes of placing the trades, Commonwealth's clearing broker-dealer detected the activity and the intruder was blocked from further trading. Commonwealth immediately canceled the unauthorized purchases and transferred them into its error account, ultimately absorbing a net loss of approximately $8,000, and reported the incident to the Commission staff. Commonwealth also notified the owners of the 368 accounts.

Commonwealth's Failure to Safeguard Customer Information and Inadequate Response to Known Deficiencies and Anticipated Security Threats

7. Regulation S-P became effective on November 13, 2000, and compliance has been mandatory since July 1, 2001. The Safeguards Rule requires that every broker, dealer and investment company, and every investment adviser registered with the Commission ("Covered Institutions"), adopt polices and procedures reasonably designed to: (1) insure the security and confidentiality of customer records and information; (2) protect against any anticipated threats or hazards to the security or integrity of customer records and information; and (3) protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer. In 2004, Regulation S-P was amended to require, among other things, that the policies and procedures Covered Institutions must adopt under the Safeguards Rule be in writing. This written safeguards policies and procedures requirement became effective on January 11, 2005, and compliance became mandatory on July 1, 2005.

8. Commonwealth had policies and procedures in place that were apparently designed to safeguard customer records and information at the time of the November 2008 intrusions. Commonwealth's written policies, which were disseminated to registered representatives via publication on Commonwealth's intranet, required each registered representative to maintain the security of the information entrusted to that person. Commonwealth was aware of the threat to the security of customer records and information and potential for unauthorized access that could result from a computer virus, based on its presentations to registered representatives concerning identity theft and several information security newsletters distributed to registered representatives. Nonetheless, while Commonwealth's policies recommended as best practices the use of antivirus software on branch office computers used by Commonwealth's registered representatives, they did not mandate antivirus software.

9. Additionally, Commonwealth did not have adequate procedures in place to follow up on potential antivirus computer security issues uncovered when registered representatives contacted Commonwealth's information technology ("IT") help desk for computer-related assistance. During the two months prior to the November 2008 intrusions, Commonwealth's IT help desk received several calls from the Commonwealth registered representative whose computer was hacked into in November 2008, indicating that the registered representative's computer system had been compromised by a software virus. On September 17, 2008, the registered representative called Commonwealth's IT help desk referencing a potential software virus problem. The order ticket maintained by Commonwealth's IT help desk for September 17, 2008 notes that Commonwealth's help desk was unable to detect antivirus software on the registered representative's computer and therefore recommended the registered representative obtain antivirus software, unless the registered representative could confirm the anti-spyware software on the computer included an antivirus component. The IT help desk did not follow up with the registered representative, and the status of the incident was changed from "open" to "waiting for reply." One day prior to the first known intrusion in early November 2008, the same registered representative again called Commonwealth's IT help desk to report additional computer problems

and the help desk employee noted that the registered representative's computer "has a major virus" and told him to take the computer to his local computer technology person to have it repaired. The registered representative brought his computer to his local technology person that afternoon, although by this time the intruder was already in possession of the login credentials necessary to access the representative's Commonwealth customer accounts.

10. Although Commonwealth's policies for customer records and information prior to the November 2008 intrusions in certain respects addressed administrative, technical, and physical safeguards for the protection of its customer records and information, by failing to require basic safeguards such as antivirus software on all Commonwealth registered representative's computers conducting business over the Internet and by failing to follow up, or have written procedures addressing the follow up, on security issues either uncovered in branch audits or reported to the IT help desk, Commonwealth failed to adhere to the standards of reasonable design imposed by the Safeguards Rule.

Violations of the Federal Securities Laws

11. As a result of the conduct described above, Commonwealth willfully[3] violated Rule 30(a) of Regulation S-P (17 C.F.R. § 248.30(a)), which requires broker-dealers and registered investment advisers to have written policies and procedures that are reasonably designed to safeguard customer records and information.

Remedial Efforts

12. In determining to accept Commonwealth's Offer, the Commission considered the remedial acts promptly undertaken by Commonwealth and the cooperation Commonwealth afforded the Commission staff.

IV.

In view of the foregoing, the Commission deems it appropriate and in the public interest to impose the sanctions agreed to in Commonwealth's Offer.

Accordingly, pursuant to Sections 15(b) and 21C of the Exchange Act and Sections 203(e) and 203(k) of the Advisers Act, it is hereby ORDERED that:

A. Respondent Commonwealth cease and desist from committing or causing any violations and any future violations of Rule 30(a) of Regulation S-P (17 C.F.R. § 248.30(a));

[3] A willful violation of the securities laws means merely "'that the person charged with the duty knows what he is doing.'" *Wonsover v. SEC*, 205 F.3d 408, 414 (D.C. Cir. 2000) (quoting *Hughes v. SEC*, 174 F.2d 969, 977 (D.C. Cir. 1949)). There is no requirement that the actor "'also be aware that he is violating one of the Rules or Acts.'" *Id.* (quoting *Gearhart & Otis, Inc. v. SEC*, 348 F.2d 798, 803 (D.C. Cir. 1965)).

B. Respondent Commonwealth is censured; and

C. Respondent Commonwealth shall, within ten (10) days of the entry of this Order, pay a civil money penalty in the amount of $100,000 to the United States Treasury. If timely payment is not made, additional interest shall accrue pursuant to SEC Rule of Practice 600. Payment shall be: (A) made by United States postal money order, certified check, bank cashier's check or bank money order; (B) made payable to the Securities and Exchange Commission; (C) hand-delivered or mailed to the Office of Financial Management, Securities and Exchange Commission, Operations Center, 6432 General Green Way, Stop 0-3, Alexandria, VA 22312; and (D) submitted under cover letter that identifies Commonwealth as a Respondent in these proceedings, the file number of these proceedings, a copy of which cover letter and money order or check shall be sent to John T. Dugan, Associate Regional Director, Securities and Exchange Commission, 33 Arch Street, 23rd Floor, Boston, Massachusetts 02110.

By the Commission.

Elizabeth M. Murphy
Secretary