

14. Add Form SP-30 (referenced in paragraph (3) of Appendix A to part 248) to read as follows:

Note: The text of Form SP-30 does not, and this amendment will not, appear in the Code of Federal Regulations.

UNITED STATES SECURITIES AND EXCHANGE COMMISSION

Washington DC 20549

FORM SP-30

SECURITY INCIDENT REPORTING FORM

(Pursuant to § 248.30(a)(4)(v) of Regulation S-P (17 CFR 248.30(a)(4)(v)))

1. Provide identifying information (IARD/CRD number, CIK,* business name, principal business and mailing addresses, and telephone number).

* CIK stands for “Central Index Key,” which is the unique number the Commission assigns to each entity that submits filings to it.

2. Provide contact employee (name, title, address, and telephone number).

3. Type of Institution:

Broker-Dealer

Investment Adviser

Investment Adviser/Broker-Dealer (Dual Registrant)

Investment Company

Transfer Agent

4. Describe the security incident (e.g., unauthorized use of your customers’ online trading accounts, unauthorized use of your employee’s password to access sensitive personal information maintained on one of your databases, or unauthorized access to your files on an investment company’s shareholders):

(a) Provide the date(s) of the incident;

(b) List Registrant's offices, divisions or branches involved;

- (c) Describe personal information system(s) compromised;
 - (d) Describe the incident and identify anyone you reasonably believe accessed or used personal information without authorization or compromised the personal information system(s).
5. Provide information on third-party service provider(s) involved:
- (a) Identify any third-party service provider involved;
 - (b) Describe the services provided;
 - (c) If the service provider is an affiliate, describe the affiliation;
 - (d) Describe the involvement of the service provider(s) in the incident.
6. Describe steps taken or that you plan to take to assess the incident.
7. Provide the number of individuals whose information appears to have been compromised: _____
8. Describe steps you have taken or plan to take to prevent improper use of any personal information that was or may be compromised by the incident.
9. Do you intend to notify affected individuals?
- (a) If yes, when?
 - (b) If no, why not?
10. Describe any steps you have taken or any plan to review your policies and procedures in light of this incident.
11. Describe Customer account losses (to the extent known)
- (a) Number of Customer Accounts Accessed: _____
 - (b) Unauthorized Money Transfers
 - (i) Initial Customer Losses from Actual or Attempted Unauthorized Transfers:
\$ _____
 - (ii) Mitigation of Customer Losses from Firm's Efforts

(A) Surveillance / Investigative Intervention: \$ _____

(B) Recoveries from Receiving Parties: \$ _____

(C) Firm Compensation to Customers: \$ _____

(iii) Net Customer Losses: \$ _____

(c) Unauthorized Changes to Securities Portfolio (e.g., Pump and Dump Schemes)

(i) Initial Customer Losses from Actual or Attempted Unauthorized Trading

(A) Value of Accounts Before the Unauthorized Trading: \$ _____

(B) Value of Accounts After the Unauthorized Trading: \$ _____

(C) Initial Customer Losses / Gains: \$ _____

(ii) Did the firm return the affected customer accounts to their positions before the unauthorized trading?

Yes / No

(iii) Net Customer Losses / Gains: \$ _____

By the Commission.

Nancy M. Morris
Secretary

Dated: March 4, 2008