

SEC Proposes Changes to Regulation S-P

Introduction

In March 2008, the SEC published proposed amendments ("Amendments") to Regulation S-P, which implements certain personal and financial privacy obligations for SEC-regulated institutions ("institutions"), such as broker-dealers and investment advisers. Regulation S-P is the implementing regulation for the Gramm Leach Bliley Act ("GLB") and the Fair Credit Reporting Act ("FCRA").

In the Amendments, the SEC would address security breaches in the securities industry by amending Regulation S-P in four principal ways:

- require more specific standards under the safeguards rule, including standards for data security breach incidences;
- broaden both the scope of the information covered and the types of institutions and persons covered under the safeguards and disposal rules;
- require covered entities to maintain written records of both their policies and procedures and their compliance with those policies and procedures; and
- create a new exception from the notice and opt-out requirements of Regulation S-P to control the flow of private investor information that commonly occurs when a representative moves from one brokerage or advisory firm to another.

Discussion

Information Security and Security Breach Response Requirements

The Amendments would require institutions to adopt an "information and security program," which entails the adoption of written policies and procedures to address administrative, technical, and physical safeguards for protection of customer records and information as well as written procedures for responding to unauthorized access to or use of personal information. The information and security program would have to be reasonably designed to: (1) ensure the security and confidentiality of personal information, (2) protect against any anticipated threats or hazards to the security or integrity of personal information, and (3) protect against unauthorized access to or use of personal information that could result in "substantial harm or inconvenience" to any consumer, employee, investor or security holder who is a natural person.

Also, the Amendments would define, for the first time, "substantial harm or inconvenience" as a "personal injury, or more than trivial financial loss, expenditure of effort or loss of time." The SEC defined the term and provided several examples in order to help clarify the scope of what would constitute "substantial harm or inconvenience" to demonstrate the term's breadth regarding types of harms covered as well as the term's aim to filter out lesser magnitudes of harm. For example, the SEC intended the definition to be broad enough to include harms other than identity theft that may result from failure to safeguard an individual's sensitive information, such as the harm that a hacker may use confidential information about an individual for extortion by threatening to make private

The period for comments to the SEC ends on May 12, 2008.

information public. Yet, the SEC does not intend for substantial harm or inconvenience to cover “unintentional access to personal information by an unauthorized person that results only in trivial financial loss, expenditure of effort or loss of time,” such as if the use of the information results in an institution deciding to change the individual’s account number or password.

The information security program would have to include particular security elements, many of which are already industry standard, to meet the requirements of Regulation S-P. Governed institutions would be required, among other things, to:

- designate in writing an employee or employees to coordinate the information security program;
- identify in writing reasonably foreseeable security risks that could result in the unauthorized compromise of personal information or personal information systems;
- design and document in writing and implement safeguards to protect identified risks;
- regularly test and monitor and document in writing the effectiveness of the implemented safeguards and procedures;
- oversee service providers and require service providers by contract to implement and maintain appropriate safeguards;
- train employees; and
- evaluate and adjust the information security program as necessary.

The Amendments would also require institutions to include written procedures for responding to incidents of unauthorized access to or use of personal information. The Amendments would include notice provisions, which would require notice to affected individuals if the misuse or possibility of misuse of personal information has occurred and notice to the SEC (or a broker-dealer’s Self Regulatory Organization (“SRO”)) in circumstances where the person has suffered substantial harm or inconvenience or intentional intrusion by someone without authorized access.

The information security program would be required to have written procedures to: assess any intrusion, including what systems were penetrated and what type of information was stolen; contain and prevent further unauthorized access; investigate and determine in writing the likelihood that the information has been or will be misused after the institution becomes aware of any unauthorized access to sensitive information; and notify individuals effected by the intrusion. The Amendments define sensitive information to include an individual’s Social Security number, or the individual’s name, telephone number, street address, e-mail address, or online user name, in combination with any one of the individual’s account number, credit or debit card number, driver’s license number, credit card expiration date or security code, mother’s maiden name, password, personal identification number, biometric authorization record, or other authenticating information.

The provision requiring notice to the SEC would not be as stringent as policies adopted by the banking agencies because the Amendments require notice to be given to the SEC only when there is a significant risk as opposed to any risk that an individual might suffer substantial harm or inconvenience. Moreover, notice to the SEC or relevant SRO would be provided on the proposed Form S-P which would include: the nature of the unauthorized access, the institution’s intended response, when the incident occurred, what offices or parts of the registrant’s business were affected, the disclosure of any third-party service providers involved, and the nature of the affiliation.

Scope of Information Covered and Expansion of Type of Persons and Entities Governed by the Safeguards and Disposal Rules

The Amendments would alter the scope of information covered as well as expand the type of persons and entities governed by the safeguards and disposal rules in an effort to create a more efficient and protective framework of privacy rules under Regulation S-P. Currently, the safeguards and disposal rules cover different information as a result of being adopted at different times under the GLB and FCRA, respectively.

The Amendments would broaden the scope of the personal information under the current different provisions into the definition of “personal information.” In addition, “personal information” would include any

information identified with any consumer, or with an employee, investor, or security holder who is a natural person, that is handled by the institution on the institution's behalf. The Amendments would also extend the safeguards and disposal rules to nonpublic personal information of employees, which would curtail the risk that an identity thief could access investor information by impersonating an employee.

The Amendments would extend the safeguards rule to govern transfer agents while limiting the scope of broker-dealers covered by the rule to those broker-dealers other than those registered by notice with the SEC under Section 15(b)(11) of the Securities Exchange Act of 1934. The SEC views extending the safeguards rule to apply to registered transfer agents as a way of streamlining the entities covered by the safeguards and disposal rules. Currently, both rules apply to brokers, dealers, registered investment advisers, and investment companies, but only the disposal rule applies to transfer agents. This proposal would amend that distinction and apply both rules across the same types of entities.

Moreover, the Amendments would limit the scope of the safeguard rules to those broker-dealers other than those registered by notice. Broker-dealers registered by notice must comply with rules for safeguarding of customer records and information adopted by the U.S. Commodity Futures Trading Commission (the "CFTC"). The purpose of the limitation is to clarify that the CFTC would maintain primary oversight and responsibility for privacy rules governing notice registered broker-dealers.

The Amendments would also extend the disposal rule to apply to natural persons who are associated persons of a broker-dealer, supervised persons of a registered investment adviser, and associated persons of a registered transfer agent.

Records of Compliance

The Amendments would require institutions governed by the safeguards and disposal rules to make and preserve written records of their safeguards and disposal policies and procedures, including documentation of compliance with the implementation, development, and maintenance of these policies and proce-

dures. The record keeping rules would also extend to incidents of unauthorized access to or misuse of personal information. To minimize compliance costs, the periods of time that an institution must preserve the records would be consistent with existing recordkeeping rules.

Exception for Notice and Opt Out Requirements

The Amendments would add a new exception to the notice and opt out requirements to permit limited disclosures of investor information when a registered representative of a broker-dealer or a supervised person of a registered investment adviser moves from one brokerage or advisory firm to another. The purpose of this exception is to create an orderly framework for controlling the type of information that departing representatives share with their new firms. The proposed exception would permit one firm by way of the moving representative to disclose to another firm only the following information: the customer's name, a general description of the type of account and products held by the customer, and contact information, including address, telephone number and e-mail information.

Departing representatives would have to provide to the firm they are leaving a written record of information that would be disclosed pursuant to the exception, and moving representatives would be barred from sharing any customer's account number, Social Security number, or securities position.

Conclusion

The Amendments add significantly to the costs and burdens of privacy protection. It remains to be seen whether the SEC will adopt them in their present form after receiving industry and other comments.



This update was authored by Robert A. Robertson (+1 949 442 6037; robert.robertson@dechert.com), Alan Rosenblat (+1 202 261 3332; alan.rosenblat@dechert.com), and Mark Goldfarb (+1 202 261 3478; mark.goldfarb@dechert.com).

Practice group contacts

For more information, please contact the authors, one of the attorneys listed, or any Dechert attorney with whom you regularly work. Visit us at www.dechert.com/financialservices.

Margaret A. Bancroft
New York
+1 212 698 3590
margaret.bancroft@dechert.com

Allison R. Beakley
Boston
+1 617 728 7124
allison.beakley@dechert.com

Sander M. Bieber
Washington, D.C.
+1 202 261 3308
sander.bieber@dechert.com

Stephen H. Bier
New York
+1 212 698 3889
stephen.bier@dechert.com

Susan M. Camillo
Boston
+1 617 728 7125
susan.camillo@dechert.com

Daphne T. Chisolm
Charlotte
+1 704 339 3153
daphne.chisolm@dechert.com

Christopher D. Christian
Boston
+1 617 728 7173
christopher.christian@dechert.com

Elliott R. Curzon
Washington, D.C.
+1 202 261 3341
elliott.curzon@dechert.com

Douglas P. Dick
Washington, D.C.
+1 202 261 3305
douglas.dick@dechert.com

Ruth S. Epstein
Washington, D.C.
+1 202 261 3322
ruth.epstein@dechert.com

Susan C. Ervin
Washington, D.C.
+1 202 261 3325
susan.ervin@dechert.com

Joseph R. Fleming
Boston
+1 617 728 7161
joseph.fleming@dechert.com

Brendan C. Fox
Washington, D.C.
+1 202 261 3381
brendan.fox@dechert.com

Wendy Robbins Fox
Washington, D.C.
+1 202 261 3390
wendy.fox@dechert.com

David M. Geffen
Boston
+1 617 728 7112
david.geffen@dechert.com

David J. Harris
Washington, D.C.
+1 202 261 3385
david.harris@dechert.com

Robert W. Helm
Washington, D.C.
+1 202 261 3356
robert.helm@dechert.com

Jane A. Kanter
Washington, D.C.
+1 202 261 3302
jane.kanter@dechert.com

Stuart J. Kaswell
Washington, D.C.
+1 202 261 3314
stuart.kaswell@dechert.com

Geoffrey R.T. Kenyon
Boston
+1 617 728 7126
geoffrey.kenyon@dechert.com

George J. Mazin
New York
+1 212 698 3570
george.mazin@dechert.com

Jack W. Murphy
Washington, D.C.
+1 202 261 3303
jack.murphy@dechert.com

John V. O'Hanlon
Boston
+1 617 728 7111
john.ohanlon@dechert.com

Fran Pollack-Matz
Washington, D.C.
+1 202 261 3442
fran.pollack-matz@dechert.com

Jeffrey S. Poretz
Washington, D.C.
+1 202 261 3358
jeffrey.poretz@dechert.com

Jon S. Rand
New York
+1 212 698 3634
jon.rand@dechert.com

Robert A. Robertson
Newport Beach
+1 949 442 6037
robert.robertson@dechert.com

Keith T. Robinson

Hong Kong
+1 852 3518 4705
keith.robinson@dechert.com

Alan Rosenblat

Washington, D.C.
+1 202 261 3332
alan.rosenblat@dechert.com

Kevin P. Scanlan

New York
+1 212 649 8716
kevin.scanlan@dechert.com

Frederick H. Sherley

Charlotte
+1 704 339 3100
frederick.sherley@dechert.com

Patrick W. D. Turley

Washington, D.C.
+1 202 261 3364
patrick.turley@dechert.com

Brian S. Vargo

Philadelphia
+1 215 994 2880
brian.vargo@dechert.com

David A. Vaughan

Washington, D.C.
+1 202 261 3355
david.vaughan@dechert.com

Anthony H. Zacharski

Hartford
+1 860 524 3937
anthony.zacharski@dechert.com



© 2008 Dechert LLP. All rights reserved. Materials have been abridged from laws, court decisions, and administrative rulings and should not be considered as legal opinions on specific facts or as a substitute for legal counsel. This publication, provided by Dechert LLP as a general informational service, may be considered attorney advertising in some jurisdictions. Prior results do not guarantee a similar outcome.

www.dechert.com

U.S. Austin • Boston • Charlotte • Hartford • Newport Beach • New York • Philadelphia
Princeton • San Francisco • Silicon Valley • Washington, D.C. • **EUROPE** Brussels
London • Luxembourg • Munich • Paris • **ASIA** Hong Kong