

# 2009

---

# NSCP

NATIONAL SOCIETY OF COMPLIANCE PROFESSIONALS INC.

EAST COAST REGIONAL MEETING

## Session III(c) GI – Privacy Considerations: Regulation SP Amendments

### **Panelists:**

*Richard C. Szuch*

Bressler, Amery & Ross, P.C.  
rszuch@bressler.com

*Miriam Lefkowitz*

Shufro Rose & Co., LLC  
mlefkowitz@shufrorose.com

*Jennifer Woods Burke*

AXA Equitable  
jennifer.burke@axa-equitable.com

### **Panel Topics:**

- Proposed Regulation SP amendments
- Information security safeguards and procedures
- Identifying, investigating and reporting on identity theft and privacy issues
- On-line account intrusions

## **I. Regulation S-P (2000)**

### **A. General Overview**

1. Regulation S-P is the SEC's existing privacy rules mandated under the Gramm-Leach-Bliley Act
2. The rule is intended to require a brokers, dealers, registered investment advisers and investment companies to:
  - a. provide notice to customers about its privacy policies and practices;
  - b. describe the conditions under which the institution may disclose nonpublic personal information about consumers to nonaffiliated third parties; and
  - c. provide a method for consumers to prevent the financial institution from disclosing that information to certain nonaffiliated third parties by "opting out" of that disclosure, subject to various exceptions as stated in the rules

### **B. Substantive Provisions**

#### **1. Privacy and Opt Out Notices**

- a. Requires delivery of initial and annual notices about the privacy policies and practices of a financial institution, and about the opportunity and methods for consumers to opt out of their institution's sharing of nonpublic personal information with nonaffiliated third parties
- b. Providing initial notices "prior to" time customer relationship is established
  - i. Initial notice must be given not later than the time when a financial institution establishes a customer relationship; not later than the time of entering an investment advisory contract with the client
  - ii. Exceptions providing for delayed delivery of initial notice when delivery either would pose a significant impediment to the conduct of a routine business practice or the consumer agrees to receive the notice later in order to obtain a financial product or service immediately
- c. Annual Notice to Customers Required
  - i. General rule requires annual notices, but a broker-dealer, fund, or registered adviser may select a calendar year as the 12-month period within which notices will be provided
  - ii. Permits a broker-dealer, fund, or registered adviser to provide annual notices to customers over the institution's web site if the customer conducts transactions electronically and agrees to the electronic disclosures
- d. Information to be Included in Initial and Annual Privacy Notices
  - i. General requirement that financial institution must provide customers with a notice describing the institution's policies and practices with respect to, among other things, disclosing nonpublic personal information to affiliates and nonaffiliated third parties
- e. Opt Out Notice to Consumers
  - i. Any opt out notice provided by a broker-dealer, fund, or registered adviser be clear and conspicuous and accurately explain the right to opt out
  - ii. Opt out election survives until revoked by the consumer

## 2. Limits on Disclosure

- a. Disclosure of Nonpublic Personal Information to Nonaffiliated Third Parties
  - i. Section 502(a) of the G-L-B Act generally prohibits a financial institution, directly or through its affiliates, from sharing nonpublic personal information about a consumer with a nonaffiliated third party unless the institution:
    - 1. Provides the consumer with a notice of the institution's privacy policies and practices;
    - 2. Provides the consumer with a clear and conspicuous notice that the consumer's nonpublic personal information may be disclosed to nonaffiliated third parties
    - 3. Gives the consumer an opportunity to opt out of that disclosure, and
    - 4. Informs the consumer how to opt out.
- b. Redislosure or Reuse of Information- only protection under the statute for a consumer who is not a customer
  - i. a nonaffiliated third party that receives nonpublic personal information from a financial institution must not, directly or indirectly through an affiliate, disclose that information to any person that is not affiliated with the financial institution or the third party, unless the disclosure would be lawful if made directly by the financial institution
  - ii. A broker-dealer, fund, or registered adviser generally may disclose nonpublic personal information to a nonaffiliated third party (i) for any purpose if the consumer has received a privacy and opt out notice and has not exercised the right to opt out, (ii) under section 502(b), and (iii) in accordance with specific enumerated exceptions under section 502(e)
- c. Limits of Sharing Account Numbers for Marketing Purposes
  - i. Generally prohibits a financial institution from disclosing, other than to a consumer reporting agency, an account number or similar form of access number or access code for a credit card account, deposit account, or transaction account of a consumer to any nonaffiliated third party for use in telemarketing, direct mail marketing, or other marketing through electronic mail to the consumer
  - ii. Exception permits a broker-dealer, fund, or registered adviser to disclose account numbers to an agent for the purpose of marketing the institution's financial product or services as long as the agent has no authority to initiate charges to the account

## 3. Exceptions

- a. Exceptions permit broker-dealers, funds, and registered advisers to disclose information to nonaffiliated third parties in circumstances such as maintaining or servicing a customer's account, or complying with federal, State, or local law
- b. Exception to the opt out requirements for service providers and joint marketing

- c. Exceptions to notice and opt out requirements for processing and servicing transactions to include disclosures made in connection with (i) servicing or processing financial products or services requested by the consumer or (ii) maintaining or servicing a customer account.
- d. Other exceptions for disclosures not made in connection with the administration, processing, servicing, or sale of a consumer's account

#### 4. Safeguard Procedures

- a. Safeguards Rule
  - i. Section 30(a) of Regulation S-P requires institutions to adopt written policies and procedures that address administrative, technical and physical safeguards to protect customer records and information
  - ii. Section 30(c) protects against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer
  - iii. The safeguards are required to be reasonably designed to meet the objectives of the Gramm-Leach-Bliley Act (“GLBA”).
- b. Disposal Rule See Disposal of Consumer Report Information, Exchange Act Release No. 50781, IAA Release No. 2332, ICA Release No. 26685 (Dec. 2, 2004), 69 FR 71322 (Dec. 8, 2004)
  - i. Requires institutions to protect against the improper disposal of consumer report information and provides that any person who maintains or possesses consumer information or any compilation of consumer information derived from a consumer report for a business purpose must properly dispose of the information.

## II. Impetus Behind Regulation S-P Amendments

- A. Challenges Posed by Information Security Breaches (ID Theft and Infiltration of Online Accounts);
- B. Broad Nature of Safeguards Rule (reasonably designed to meet GLBA’s objectives)
- C. Concern About Scope of Information Covered
- D. Address the Issue of Reps Moving to Another Firm
- E. Commission’s Desire to More Closely Align its Privacy Guidelines with Those of the Federal Trade Commission (“FTC”) and the Federal Banking Agencies, which Adopted Data Breach Notice Rules in 2005.

### III. Proposed Reg S-P Amendments (proposed March 4, 2008- remain unadopted)

#### A. Major Subparts of Proposed Amendments

##### 1. Information Security and Security Breach Response Requirements

###### a. Revised Safeguarding Policies and Procedures

- i. Would require each institution subject to the safeguards rule to develop, implement, and maintain a comprehensive “information security program,” including written policies and procedures that provide administrative, technical, and physical safeguards for protecting personal information, and for responding to unauthorized access to or use of personal information
- ii. The information security program must be reasonably designed to:
  1. ensure 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 customer, employee, investor or security holder who is a natural person
    - a. Substantial harm or inconvenience would be defined as “personal injury, or more than trivial financial loss, expenditure of effort or loss of time.”
- iii. Institutions subject to the rule would be required to:
  1. designate in writing employee(s) to coordinate the information security program;
  2. identify in writing reasonably foreseeable security risks that could result in unauthorized disclosure, misuse, alteration, destruction or other compromise of personal information (systems);
  3. design and document in writing and implement information safeguards to control the identified risks;
  4. regularly test or monitor and document in writing the effectiveness of the safeguards’ key controls, systems, and procedures, including the effectiveness of access controls on personal information systems, controls to detect, prevent and respond to attacks, or intrusions by unauthorized persons, and employee training and supervision;
  5. train staff to implement the information security program;
  6. oversee service providers by taking reasonable steps to select and retain service providers capable of maintaining appropriate safeguards for the personal information at issue, and require service providers by contract to implement and maintain appropriate safeguards (and document such oversight in writing); and
  7. evaluate and adjust their information security programs to reflect the results of the testing and monitoring, relevant technology changes, material changes to operations or business arrangements, and any other circumstances that the institution knows or reasonably believes may have a material impact on the program

###### b. Data Security Breach Response

- i. Proposing that information security programs include procedures for responding to incidents of authorized access or to use of personal information

- ii. Procedures would include notice to affected individuals, SEC (or for broker-dealers, their designated examining authority) through use of a proposed form if any incident of unauthorized access to or use of personal information where there is a significant risk of substantial harm or inconvenience, or where an unauthorized person intentionally obtained access to or used sensitive personal information.
- iii. Institutions subject to the rule would be required to have written procedures to:
  - 1. assess any incident involving unauthorized access or use, and identify in writing what personal information systems and what types of personal information may have been compromised;
  - 2. take steps to contain and control the incident to prevent further unauthorized access or use and document all steps taken in writing;
  - 3. promptly conduct reasonable investigation and determine in writing the likelihood that the information has or will be misused after the institution becomes aware of any unauthorized access to sensitive personal information; and
  - 4. notify individuals with whom the information is identified if institution determines misuse of information or such misuse is reasonably possible (and document in writing); specific requirements for notices to affected individuals proposed

## 2. Scope of the Safeguards and Disposal Rules

- a. Information covered by the safeguards and disposal rules (currently different information subject to the two rules)
  - i. Proposal broadens the scope of information protected by both the safeguards rule and the disposal rule
- b. Safeguards and disposal rule amended to protect “personal information” and to define that term to include any record containing either “nonpublic personal information” or “consumer report information” (each of those terms are defined in Reg S-P)
  - i. Consumer Report Information- any record about an individual that is a consumer report or is derived from or is a compilation of such records, not including information that does not identify individuals (aggregate or blind information)
  - ii. “Personal Information” also includes “information identified with any consumer or with any employee, investor, or securityholder who is a natural person, in paper, electronic or other form that is handled by the institution or maintained on the institution’s behalf.”
- c. Proposed amendments would apply safeguards and disposal rules to nonpublic personal information or consumer report information that is identified with any individual, consumer, employee, investor or securityholder and handled or maintained by or on behalf of the institution
- d. Institutions Covered by the Safeguards Rule
  - i. Safeguard rule currently applies to brokers, dealers, registered investment advisors, and investment companies

ii. Proposal to extend safeguards rule to **registered transfer agents** (as defined in Section 3(a)(25) of the Exchange Act (15 U.S.C. 78c(a)(25)), because they have exposure to sensitive personal information

e. Persons Covered by the Disposal Rule

i. Disposal rule currently applies to broker-dealers, investment companies, registered investment advisors and registered transfer agents.

ii. Proposal to extend disposal rule to apply to **natural persons** who are associated persons of a broker or dealer, supervised persons of a registered investment advisor, and associated persons of a registered transfer agent.

3. Records of Compliance

a. Proposal to require institutions subject to safeguard and disposal rules to maintain written records of their safeguards and disposal policies and procedures

b. Proposal to require that institutions document compliance with developing, maintaining and implementing these policies and procedures for protecting and disposing of personal information

c. Preservation requirements would be consistent with existing recordkeeping rules, in requiring preservation of records:

i. Broker-dealers- for not less than **three years**, the first two in an easily accessible place

ii. Registered transfer agents- for not less than **two years**, the first year in an easily accessible place

iii. Investment companies- for not less than **six years**, the first two years in an easily accessible place

iv. Registered investment advisors- for **five years**, the first two years in an appropriate office of the investment advisor

4. Exception for Limited Information Disclosure When Personnel Leave Their Firms

a. Proposed new exception from notice and opt out requirements to permit limited disclosure 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

b. Proposal would allow firms with departing representatives to share limited customer information with the representative's new firm that could be used to contact clients

c. Broker-dealers and registered investment advisers seeking to rely on this exception must require their departing representatives to provide to them, not later than the representative's separation from employment, a written record of the information that would be disclosed pursuant to the exception, and the broker-dealer and registered investment advisers would be required to preserve such records consistent with the proposed recordkeeping provisions of Section 30.

- d. The proposed exception would permit one firm to disclose to another only the following information:
  - i. Customer's name
  - ii. General description of the type of account and products held by customer
  - iii. Contact information- address, telephone and email information
- e. Shared information could NOT include:
  - i. Customer account numbers
  - ii. Social Security number
  - iii. Securities positions
- f. A representative could solicit only an institution's customers that were that representative's clients

#### **IV. Concerns Posed by Proposed Reg S-P Amendments**

- A. Expanded Scope of Information Covered by the Rules
  - 1. Whether this definition of "personal information" is too broad and if such a definition would make implementation impracticable or would impose undue expense
- B. Inconsistency in Standards for "Substantial Harm or Inconvenience" Under Safeguards Rule Between SEC and Other Regulators
  - 1. The proposed amendments define "substantial harm or inconvenience" to mean "personal injury, or more than trivial financial loss, expenditure of effort, or loss of time."
  - 2. There are concerns that this definition is narrower than guidance issued by banking regulators and the Federal Trade Commission ("FTC"), which use the term "substantial harm or inconvenience" as a factor in their information security rules but have not defined the phrase.
  - 3. This potential conflict is particularly relevant to larger financial service firms having a high degree of integration between their banking and securities businesses because they may now have to deal with inconsistencies in complying with two or more different information safeguarding standards.
- C. Burden on Covered Companies
  - 1. The expansion of scope of individuals and information covered would place additional burdens on financial institutions of increased cost, oversight and staffing to ensure compliance.
  - 2. Firms would be required to designate the employees responsible for the information covered by the safeguards and disposal rules
  - 3. The proposed amendments would create added expenses and enhanced regulatory requirements for covered companies
- D. Cost of Compliance
  - 1. The SEC estimates smaller firms would have to spend 2 to 80 hours and an average of \$18,560 initially to adopt the enhanced procedures; Larger firms are expected to spend between 40 and 400 hours and an average of \$172,732 to adopt and implement the new procedures
  - 2. Annual compliance for small firms is estimated by the SEC to involve 12 to 40 hours and an average annual cost of \$10,764; larger firms are expected to need

32 to 100 hours for compliance annually, at an estimated average yearly cost of \$51,084.

3. Many firms indicate that these figures are at low end and that their expected costs would be higher

#### E. Providing Notice to Customers and SEC or SRO

1. Threshold Too Low- commentators have questioned whether the SEC should require notice to customers each time an unauthorized person has obtained access to or used sensitive personal information if there is no significant risk of substantial harm or inconvenience to the individual
2. FINRA submitted a comment in which it stated that notice to FINRA would often prove ineffectual because FINRA or the SRO will often have limited jurisdiction to take significant action against the perpetrators (where those perpetrators were non-associated persons of a member firm).

#### F. State Security Breach Laws May Conflict with the Proposed Amendment

1. A new federal requirement may result in the duplication of notifications to clients who reside in states with substantially different requirements than those imposed by the proposed amendment

#### G. Private Cause of Action

1. The proposed amendments may give rise to a private cause of action for a firm's failure to have an Information Security Program that meets the requirements or if the firm fails to follow the terms of their program.
2. Comments suggest changing proposal to clearly state that there is no private cause of action.

#### H. Increased Individual Liability

1. The proposed amendment creates individual liability for violations by expanding the safeguard rules to include associated persons of broker-dealers and supervised persons of investment advisers.
2. This would increase the liability exposure for broker-dealer employees and financial advisors- they will look to their firm for higher compensation or insurance coverage to offset the risk, while the costs will be passed on to clients.

#### I. Easing of Restrictions on Covered Companies

1. Ease existing restrictions on firms recruiting registered representatives by allowing representatives who switch firms to disclose certain client information without having to comply with the usual notice and opt-out rules under Regulation S-P
2. Would reduce the burdens on representatives by permitting them to use certain information to solicit clients for their new firm.
3. Broker-dealers have commented that this exception undermines their authority to maintain policies, employment contracts and other mechanisms to prohibit or permit the use of customer information
4. Note that firms may still establish a policy of precluding the transfer of information by departing registered representatives- (creates a veto power by the registered representative's original firm)

# **Sample Forms and Language Provided by Miriam Lefkowitz**

**NOTE: These samples are representative of the types of forms and clauses you might wish to use.  
They may not be suitable or appropriate for any particular firm or situation and may not  
address all relevant issues.**

**BROKER NAME**  
**Annual Confidentiality Certification**

I further understand that I will become aware of confidential information while working at BROKER and I am prohibited from divulging or communicating this information both during and after my employment. I will not disclose confidential information to other BROKER employees who do not require such information in furtherance of their duties to BROKER or to persons or businesses outside of BROKER, such as friends, immediate family members, other relatives, clients, prospects, vendors or competitors.

I agree to respect the firm's and its clients' right to confidentiality and privacy. I acknowledge that I must protect BROKER's confidential and business information and make efforts to handle it carefully and during the business day as well as securing it appropriately at the end of the business day.

I agree not to use, disseminate or disclose any confidential information, except where authorized previously by BROKER. I understand that BROKER's information is a corporate asset and that BROKER protects its confidential information to the fullest extent to the law.

I agree to return to BROKER all property then in my possession or custody and belonging to BROKER, including any confidential information, if so requested by BROKER, at any time, both during and after my employment.

I further agree to notify \_\_\_\_\_ promptly if I learn of any actual or suspected breaches of these obligations, or failures by any current or former employees or vendors, to protect the confidentiality of BROKER's confidential information.

\_\_\_\_\_  
Name (print)

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Date

**BROKER NAME**  
**Outside Vendor Confidentiality Agreement**

I understand that \_\_\_\_\_ (company name) (“Vendor”) may become aware of confidential information while performing work for BROKER NAME (“BROKER”). “Confidential information” includes, but is not limited to: all information or material that is not in the public domain and that is disclosed or otherwise made available by BROKER to Vendor or that comes to Vendor’s attention from BROKER, such as the identity of, and all information related to BROKER’s clients; any passwords used by BROKER or any of its employees; BROKER’s organization, financial structure, and financial condition; BROKER’s assets and liabilities; intellectual property, operations, interests, and plans and current or future business plans and models, regardless of whether such information is designated as “Confidential Information” at the time of its disclosure

Vendor agrees that it shall observe all commercially practicable standards of care in handling, distributing, storing and disposing of information relating to BROKER. Vendor further agrees that it will undertake to train all of the employees or agents who will be performing work on behalf of BROKER recognize and adhere to these rules.

1. Confidential BROKER information may not be disclosed to anyone, including other employees of Vendor or of BROKER, except to the extent such parties require such information in furtherance of their duties relating to BROKER.
2. Vendor shall respect BROKER and its employees and clients’ right to confidentiality and privacy.
3. Vendor must protect all BROKER confidential information and make efforts to handle it carefully as well as securing and disposing of it appropriately.
4. Vendor must return to BROKER all property then in Vendor’s possession or custody and belonging to BROKER, including any confidential information, if so requested by BROKER.
5. If requested by BROKER, Vendor periodically shall certify to BROKER that it has abided by these rules.
6. Vendor agrees to notify BROKER’s general counsel promptly if it learns of any actual or suspected breaches of these obligations or failures by Vendor to protect the confidentiality of BROKER’s confidential information.

By signing below, you warrant that you have authority to bind Vendor and the ability to adhere to these obligations.

**Vendor:** \_\_\_\_\_

**Date:** \_\_\_\_\_

By (name and title):

**BROKER NAME**  
**Non-Employee Confidentiality Agreement**

I, \_\_\_\_\_, have been engaged to provide certain services to BROKER NAME (BROKER).

I understand that I may become aware of confidential information while performing work on behalf of BROKER. "Confidential information" includes, but is not limited to: all information or material that is not in the public domain and that is disclosed or otherwise made available by BROKER to me or that comes to my attention from BROKER, such as the identity of, and all information related to BROKER's clients; BROKER's organization, financial structure, and financial condition; BROKER's assets and liabilities; operations, interests, and plans and current or future business plans and models, regardless of whether such information is designated as "Confidential Information" at the time of its disclosure.

Confidential information may not be disclosed to other employees who do not require such information in furtherance of their duties to BROKER or to persons or businesses outside of BROKER, such as friends, immediate family members, other relatives, clients, prospects, vendors or competitors. Misusing confidential information may violate state and federal privacy laws. I have reviewed BROKER's Privacy Policy and will not take or permit to be taken any action which will cause BROKER to violate its policy.

I agree to respect the firm's and its clients' right to confidentiality and privacy. I understand that I am prohibited from divulging or communicating confidential information both during and after the assignment period. I acknowledge that I must protect BROKER's confidential and business information and make efforts to handle it carefully during the business day as well as securing it appropriately at the end of the business day. I further agree to access client information only as permitted in the performance of my duties or as otherwise directed by the firm.

Upon completion of my assignment at BROKER, I agree to return to BROKER all property then in my possession or custody and belonging to BROKER, including any confidential information. Any new code, changes to existing code, software applications, documentation or materials developed during the course of the assignment shall become the sole property of BROKER, who shall retain exclusive use and/or rights to such material. I further agree that I may not retain any copies or reproductions of code, correspondence, memoranda, reports, projections, notes, financial information, or other documents relating in any way to the affairs of BROKER and its clients, other than publicly filed documents, unless I receive prior written permission from \_\_\_\_\_.

I understand that (1) BROKER shall have no adequate remedy in money or other damages in the event of a breach and, accordingly shall be entitled to injunctive relief in the event of a breach or threatened breach, and may also sue to recover an amount equal to the damages caused by the breach and the revenues I, or anyone acting in concert with me, derived from the breach, together with all remedies permitted by law or equity; (2) BROKER's waiver of a breach of this Agreement does not constitute a waiver of any prior or subsequent breach; and (3) if any of the provisions of this Agreement are found to be unenforceable, the remainder shall be enforced as fully as possible and the unenforceable

provision(s) shall be deemed modified to the limited extent required to permit enforcement of the Agreement as a whole.

<b>BROKER</b>	<b>Consultant/Temporary Employee</b>
_____	_____
Representative Name (print)	Representative Name (print)
_____	_____
Title	Title (if any)
_____	_____
Signature	Signature
_____	_____
Date	Date

These are some clauses that a small broker dealer recently inserted into its agreement with a national provider of off-site storage facilities and document destruction services. The vendor offered many services, which included retrieving individual files from boxes in storage, which files could then be faxed to the broker. Historically, this service had been very convenient for the administrative staff at the BD, and saved the BD money on having boxes delivered back and forth to the BD.

Upon a privacy review by counsel, the BD updated its agreement with its vendor, terminated the vendor's authority to access any of the files in the BD's boxes, and inserted the following clauses into the vendor's master service agreement.

1. RECORDS STORER acknowledges that it has no authority to open any of the cartons provided to it by BROKER.
2. As disclosed in RECORDS STORER's Privacy Policy, a copy of which is appended to this Service Agreement, RECORDS STORER warrants that it will manage Broker's documents and information in accordance with the securities regulations governing privacy and confidentiality of customer information.
3. RECORDS STORER shall use the same degree of care to safeguard Confidential Information as it utilizes to safeguard its own confidential information, but in no case less than reasonable care. Reasonable care shall include limiting access to BROKER's documents to employees or agents who have valid business reasons to access them at such time as the access is permitted.
4. In the event that there is a breach of confidentiality with respect to BROKER's records, or, if appears reasonably certain that there has been such a breach, RECORDS STORER shall notify BROKER, in writing, as soon as practicable, but in no event later than 48 hours after discovery, even if the scope of the breach has not yet been determined. RECORDS STORER shall also timely notify BROKER if (i) any of its employees or subcontractors who have had access to BROKER's documents are terminated for cause, if such cause relates to violating privacy of any records entrusted to RECORDS STORER, by any client; (ii) any of its employees or subcontractors who have had access to BROKER's documents are convicted or violating any state or federal law relating to privacy or fraud
5. RECORDS STORER shall not subcontract any services to be performed for BROKER, or permit access to BROKER's Deposits, to any subcontractor, unless such subcontractor maintains a privacy policy, and engages in practices, which satisfy the requirements of the federal securities laws and regulations. RECORDS STORER will remain liable for all services performed for Customer.
6. RECORDS STORER acknowledges that (i) BROKER is a regulated entity under the Securities Exchange Act of 1934 and the Investment Adviser's Act of 1940; (ii) BROKER is subject to certain records retention requirements as a regulated entity; (iii) BROKER intends to use RECORDS STORER to satisfy some of those records retention requirements; and (iv) BROKER will be held accountable to various regulatory agencies in the event that RECORDS STORER fails to meet its obligations under this contract. Accordingly, BROKER reserves the right to monitor RECORDS STORER's performance of those terms, including to seeking periodic certifications that there have been no breaches of confidentiality.