

## **PRIVACY – COMMENTS AND PERSPECTIVE ON PRIVACY PROGRAMS**

*By Barry Hollander*

With the proliferation of identity theft, the imposition of new regulations regarding the protection of nonpublic consumer personal information, and the increased focus by regulators on privacy matters during examinations, financial institutions are beginning to reevaluate the privacy policies and procedures they have in force which are intended to protect such information.

Firms must assess every aspect of their policy beginning with identifying what information needs to be protected to the eventual disposal of that information.

This paper will discuss guidelines for developing and implementing a privacy program, including the process for conducting a risk assessment of a firm's privacy program as well as new regulatory developments in the area of privacy safeguards.

### **FROM A TO Z – A SYSTEMATIC APPROACH TO DEVELOPING A PROGRAM FOR PROTECTING CLIENT INFORMATION.**

#### **I. Identify the Information - What types of information need to be protected?**

Regulations such as SEC's Regulation S-P and the new Red Flag Rule promulgated by the Federal Trade Commission and the Treasury Department are applicable to certain financial institutions and are intended for the protection consumer personal information. Examples of such information are account numbers, social security numbers and any financial information that a customer provides to a firm in the course of acquiring a financial product. Despite the rules' applicability to individuals, it is appropriate to apply many aspects of the safeguards not only to individual clients but to non-individual clients as well because non-individual clients expect that their information be protected and the firm may be bound contractually to protect such information.

#### **II. Assess the risks:**

All firms must assess the particular risks associated with all types of communications and documentation whether they are electronic, written or oral. The assessment must include a comprehensive understanding of:

1. How information is received by the firm;
2. Once received how is that information:
  - a. Stored;
  - b. Accessed; and
  - c. Used.
3. How the information is transmitted by the firm to third parties.

Once the firm has an understanding of the receipt, storage, use and transmission of information, it must then identify the vulnerabilities inherent in all those aspects.

**Electronic:**

With the expanding reliance on communication and documentation through electronic means, firms must continually be educated as to the risks associated with communicating and storing information electronically. Firms should be realistic in their approach to electronic communications. Because in most cases monitoring of 100% of the electronic communications of personnel is impossible, firms should create education programs to inform their staff as to the importance of firm policies.

Each of the information and communication platforms utilized by a firm carries its own particular risks. Consider the following:

1. Office environment: Firms must assess the security of the electronic systems in the work environment. Information technology is often outsourced and due to limited resources, firms may not have the most up to date security systems necessary to protect information. Firms must ensure that their systems are protected from:
  - a. intrusion by hackers who may have malicious or mischievous intentions;
  - b. internal sabotage and viruses;
  - c. Hardware and software bugs;
  - d. Business disruptions; and
  - e. Technological and human error.

It is imperative that resources be dedicated to ensuring that the office environment is not subject to disruption for any of the reasons above. Firms should also evaluate which personnel have access to information and assess whether the permissions granted are too broad, or simply stated are permissions granted on a “need to know” basis?

Larger firms have engaged the services of consulting firms solely for the purpose of assessing the appropriateness of access of company personnel to sensitive information. Another consideration is the firm's policy regarding the use of removable media such as CDs, DVDs, and flash drives.

In addition, firms who share nonpublic consumer personal information with third party service providers must conduct due diligence to have assurance that those parties have adequate privacy policies, procedures and systems in force.

2. Blackberries, PDAs and Cell Phones: The use of portable devices has changed the financial industry, allowing people to conduct business from remote locations and the expanded functionality of these devices has also increased the risks of compromising client information. Many of the devices allow the user to have more than one email platform on them, thereby allowing the user to communicate to and about clients through platforms that are not monitored by the firm, hence not subject to the company's supervision, scrutiny and security. Also some devices allow pin to pin and text message communications, again not afforded the protection of the of the firm's systems.

3. Laptops and non-firm owned computers: Companies have increased their flexibility in allowing employees to work at home, but many issues arise with working from remote locations and from the use of non-company owned computers, and the ability to download sensitive information on non-company owned computers and print such information in a remote location:

- a. Employees who work from home may be using wired or wireless networks without adequate firewalls and the work area may be in a location where unauthorized persons may have access;
- b. Those who travel may be using hotel or airport networks which may be targets of hackers;
- c. One should consider what happens to the information once it is downloaded at the remote location:
  - i. Is it printed, and if so how is it disposed of and who may have access to the printed information if it is left on a desk?
  - ii. Is the information left on the computer monitor and viewable by unauthorized persons?

### **Hard Copy Correspondence**

Many issues arise as to the receipt and transmission of hard copy correspondence and how those documents are maintained.

A few questions that need to be examined:

1. Are the files which hold written information kept in a secure area and is access restricted on a need to know basis?
2. Do employees leave files on their desks after working hours? Numerous cases of identity theft have taken place as a result of sensitive information being left unprotected on an employee's desk.
3. Who is authorized to disseminate information to third parties and regulators?
4. What assurances does the company have with regard to the privacy policies and procedures of third party service providers who have access to such information?

### **Oral Communications**

Understandably, it is difficult to monitor what employees say. However, it should be clearly enumerated from initial hire and through periodic training that employees should always be mindful of the environment in which they are communicating and sensitive to what information they are discussing with clients, fellow employees or third parties.

## **III. Establish the Safeguards**

Once the company has assessed the risks associated with the receipt and transmission of communications containing client information and those risks associated with maintenance and use of the information, it should implement safeguards against those risks. Below are safeguards broken down into two categories; physical and electronic. Firms should consider these safeguards and apply them as appropriate.

### **Physical Safeguards:**

1. Restrict information in the company's files, and other Customer account documents to such persons as the compliance department deems as needing to know the information;
2. When engaging in telephone conversations with customers or other authorized persons, require password authorization or other verification methods to release non-public personal in the conversation;
3. Enforce a policy which ensures that any requests for customer information received by the company from outside parties, such as regulators, the IRS and other government or civil agencies, are referred to the compliance for review;
4. If applicable, ask for the results of clearing firms' testing covering security of customer information and/or obtain certifications from the clearing firm that testing was conducted and no material inadequacies were uncovered;
5. Ensure that Customer Nonpublic Personal Information is provided to non-affiliated third parties by written agreement only;
6. Ensure that all agreements with all third-party service providers include the third party's privacy policies and ensure that those policies are adequate;
7. If required by state law, notify states if Customer information is stolen, thereby making it subject to potential identity theft;
8. Develop secure methods of disposal of customer information (see discussion below);
9. Have each employee sign an acknowledgement that they have received, read, understood and agree to be bound by the privacy procedures; and
10. Ensure that hard copies of a Customers' Nonpublic Personal Financial Information are maintained in the Company's central files, and are secured (locked) after normal business hours. In addition, Firms should consider a "clean desk policy" or some other methods of securing client information e.g. desktop secure files.

### **Electronic Safeguards**

1. Access to computerized information is permitted only through passwords or other established controls within the firm's or third party's system to ensure that only authorized personnel gain access;
2. Ensure that the firm's website will not include any non-personal financial information about customers or former customers;
3. Ensure that the firm maintains a secure server and adequate firewalls and virus protection;
4. Ensure that employees and other persons associated with the firm are not allowed to download or print sensitive information, including Nonpublic Personal Information, to their desktop, laptop computers or printers without specific authorization by compliance;
5. Ensure that firm employees working outside the office will obtain access to the firm network only with prior permission and after obtaining confirmation and authentication;
6. Ensure that firm employees working outside the office will maintain adequate firewalls and virus protection on their computers prior to obtaining access to the firm's network;
7. Ensure that firm employees desiring to use wireless fidelity ("Wi-Fi") to access Customer information must do so on the firm's premises or receive prior approval from compliance and ensure that they maintain required firewalls or other approved protection on their computers; and
8. Ensure that any Nonpublic Personal Information is only available through communication platforms that are subject to archiving by the Firm's supervisory personnel.

### **IV. DISPOSING OF CLIENT INFORMATION**

Firms are subject to regulations regarding the period in which certain information must be retained. In addition, firms may move such information from one type of storage medium to another. At the point where the information no longer has to be retained or alternate media are used for the maintenance of the information, appropriate disposal methods must use for

the information. Firms should have procedures covering the following areas:

1. Systems to identify and document the information to be destroyed;
2. Appropriate methods of disposal such as shredding of both hard copy and electronic media; and
3. Consideration of methods of destroying information that is transmitted to third party

## **V. MONITOR, TEST and TRAIN**

### MONITOR:

In order for any program to be effective it must be constantly monitored. Particularly in the area of technology, firms must be aware of developments that may render their current system out of date and jeopardize the security of sensitive information. Firms should also be mindful of the changes in their business which may give rise to additional risks. Accordingly, firms must ensure that their systems and risk assessments are up to date either through in-house staff or outside consultants.

### TEST:

Periodically, compliance should test the adequacy of the firm's physical and electronic safeguards. These tests should include both the physical and electronic safeguards and disposal methods. Firms should document the results of the review and all steps taken to update the program.

### TRAIN:

Firms should provide training on the policies and procedures as well as regulatory requirements for safeguarding of information. The frequency of such training should be assessed and modified as appropriate. In addition, those employees involved in information technology should receive additional training, where necessary, as new technologies emerge that may impact the firm's responsibilities regarding privacy of customer information.

|

## NEW REGULATORY DEVELOPMENTS

### I. THE “RED FLAG” RULE

#### 1. What is the red flag rule?

Identity thieves use people’s personally identifying information to open new accounts and misuse existing accounts, creating havoc for consumers and businesses. As a result, the Federal Trade Commission and federal bank regulatory agencies have issued regulations known as the Red Flag Rules which require certain financial institutions to identify, detect and respond appropriately to warning signs or red flags.

November 1, 2008 was the deadline for financial institutions subject to the rule, which includes certain broker-dealers, to enact red flag identity theft prevention programs. Firms must update their privacy to comply with the rule.

#### 2. What is required?

There is no set blueprint that must be followed, but essentially the requirement is that each firm must develop and implement a written identity theft prevention program which is designed to detect, prevent and mitigate identity theft in connection with both new and existing accounts of the firm. The policy may be integrated with the firm’s current privacy policy. The basic elements of the plan must include provisions for the following:

- a. Identifying relevant red flags and include those red flags into the program
- b. Detecting the red flags that have been incorporated into the program
- c. Responding appropriately to any detected red flags to prevent and mitigate ID theft; and
- d. Ensuring that program is reviewed and updated periodically to reflect changes and risks to customers

All firms must first choose the red flags that are to be incorporated into their programs. These red flags should be appropriate for the particular business of the firm. Regulators have identified 26 red flags which fall into the following broad categories:

- a. Alerts, notifications or other warnings received from consumer reporting agencies or service providers such as fraud detection services
- b. Presentation of suspicious documents
- c. Presentation of suspicious personal identifying information
- d. Unusual use of an account or other suspicious activity in the account
- e. Notices from customers, victims of ID Theft, law enforcement authorities or other persons regarding possibility of identity theft

Once the red flags have been identified in your procedures, the procedures must address the appropriate responses to the red flags once detected. These would include monitoring an account, contacting the customer or in the case of a new account application where a red flag has been detected, not opening the account.

## **II. PROPOSED AMENDMENTS TO REGULATION S-P**

In an effort to help prevent identity theft of securities industry customers, and in light of well-publicized instances of securities firms losing client information, whether it be data tapes or laptops containing sensitive information, failing to dispose of such information properly, and instances of hacking into customer accounts, on March 4, 2008, the SEC announced proposed changes to its Regulation S-P.

The SEC has proposed to substitute the current general requirement that a financial institution adopt written policies and procedures that address administrative, technical and physical safeguards to protect customer records and information, with the proposed rules which would require each institution 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 the unauthorized access to or use of personal information.

Security programs under the proposed rules must be reasonably designed to ensure the security and confidentiality of personal information, protect against any anticipated threats or hazards to the security and integrity of personal information, and protect against unauthorized access to or use of personal information that could result in substantial harm or inconvenience to any consumer, employee, investor or securityholder who is a natural person.

The rule, among other things, will require firms to:

1. Designate an employee or employees to coordinate the information security program;
2. Perform a written risk assessment and design the program to control the identified risks;
3. Regularly test and monitor the effectiveness of the safeguards' key controls, systems and procedures, including the effectiveness of access controls on personal information systems and controls to detect, prevent and respond to attacks or intrusions by unauthorized persons;
4. Adjust those controls and procedures as appropriate in light of that testing and monitoring, as well as 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;
5. Provide training to employees on the information security program; and
6. Ensure that service providers engaged by the firm have implemented and maintained appropriate safeguards for personal information the firm shares with those service providers.

In addition, because of its concerns about the potential harm to individuals when a data security breach occurs, the SEC also proposed to require information security programs to include procedures for responding to incidents of unauthorized access to or use of personal information as follows:

1. In the event a data security breach occurs, the proposal requires institutions to "take appropriate steps to contain and control the incident ... and maintain a written record of the steps [taken]" and to "conduct a reasonable investigation, determine the likelihood that the information has been or will be misused, and maintain a written record of [that] determination."
2. The firm's procedures would have to include providing prompt notice to affected individuals if misuse of "sensitive personal information" has occurred or is reasonably possible, as well as providing prompt notice to the SEC if an individual has suffered "substantial harm or inconvenience"

or an unauthorized person has intentionally obtained access to or used “sensitive personal information.”

3. The notice to the SEC would require the filing of a new proposed form, Form SP-30. Among other things, proposed Form SP-30 requires customer account losses, to the extent known, to be quantified.

### **III. THE LPL CASE – HOW NOT TO HANDLE SAFEGUARDING ISSUES**

Recently, the SEC sanctioned LPL Financial Corporation, a broker-dealer, investment adviser and transfer agent for failing to adopt policies and procedures under Rule 30 of Regulation S-P to safeguard customers’ personal information.

While not admitting or denying the findings of the SEC, LPL agreed to:

1. Censure
2. A fine of \$275,000
3. Cease and desist from further violations
4. Retain an independent consultant to:
  - a. Review and revamp their policies and procedures; and
  - b. Train employees on safeguarding matters

Between July 2007 and early 2008 hackers accessed LPL’s online trading platform for registered representatives and attempted to place unauthorized trades in the value of over \$700,000. While most of the efforts were unsuccessful, the firm reimbursed customers for approximately \$100,000 in losses resulting from the unauthorized trades.

All this occurred after LPL had conducted an internal audit that had warned of deficient security controls and the potential exposure to hackers. The audit estimated the cost of implementing an updated security system at approximately \$500,000, which probably was less than LPL’s outlay when taking into account the fines, reimbursement to customers, legal and consulting costs.

LPL had properly identified their risk and simply failed to act on it.

#### **SUMMARY:**

Upon review of the material above, one will find that there is overlap between the some of the suggestions for developing a risk assessment program and the requirements under the “Red Flag” Rule and the proposed amendments to Regulation S-P. Compliance should review the materials and determine the required areas of focus and arrive at a unified program which addresses all the relevant risks and rule requirements.

*Barry Hollander is the Senior Consultant in New York for Securities Compliance Advisors, LLC and a victim of identity theft.*