Notice to Members

JULY 2005

SUGGESTED ROUTING

Internal Audit
Legal & Compliance
Operations
Senior Management
Systems
New Technology

KEY TOPICS

Privacy
Protection of Customer Information

GUIDANCE

Safeguarding Confidential Customer Information

NASD Reminds Members of Their Obligations Relating to the Protection of Customer Information

Executive Summary

NASD members are required to maintain policies and procedures that address the protection of customer information and records. Among other things, these policies and procedures must be reasonably designed to protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer. This *Notice* reminds members of their obligation to maintain policies and procedures that are intended to protect customer information and to ensure that their policies and procedures adequately reflect changes in technology or alternative work arrangements.[1]

Questions/Further Information

Legal questions or comments concerning this *Notice* may be directed to the Office of General Counsel, Regulatory Policy and Oversight, at (202) 728-8071.

Background

Under Securities and Exchange Commission (SEC) Rule 30 of Regulation S-P, members, as well as other financial institutions, are required to adopt written policies and procedures that address the protection of customer information and records.[2] Specifically, the policies and procedures must be reasonably designed to:

(1) ensure 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.

Thus, members must be mindful of the importance of safeguarding customer information. This *Notice* reminds members of their obligation to protect confidential customer records and information and provides two examples of the types of technological or other changes that may implicate a member's duty to protect customer information and the issues the member should consider in connection with those changes.

Recent Developments

Within the past several years, there have been numerous technological advancements and other changes in the workplace that may raise concerns regarding the safeguarding of customer information. For example, an increasing number of individuals across all sectors of the workforce, including the financial services industry, are now telecommuting or working part-time from their homes or while on travel.[3] The increased use of laptops and wireless email devices, for example, provide employees with numerous alternative work arrangements. While these new methods of working and communicating are often beneficial to both employers and employees, they can present concerns for the privacy of customer information that members should keep in mind. This Notice addresses two increasingly widespread issues: wireless technology and remote access to information.[4]

Wireless Fidelity (Wi-Fi)

One relatively recent advance in technology that is being more widely embraced with each passing year is the use of wireless fidelity, or "Wi-Fi." While Wi-Fi is a generic term used to refer to various types of wireless networks, it often refers to wireless connectivity to the Internet. This connectivity can take several forms. For example, many people have wireless capabilities in their homes, and some telecommunications vendors now offer wireless Internet connectivity that is as broad-based as cell phone coverage, which can allow people to connect wirelessly to the Internet from anywhere within the coverage area (*e.g.*, an entire city). In addition, people can also tap into a wireless Internet connection in some business establishments (*e.g.*, hotels, coffee shops, and Internet cafes).

There are at least two major issues members should consider if they allow their associated persons to use wireless technology when servicing customer accounts. The first is that the data is broadcast out into the airwaves, thus making any confidential information in that data easier to intercept than if the user is required to tap into a physical wire. This is why the use of appropriate safeguards, for example encryption, is important to help prevent unauthorized parties from accessing the data.

Another issue raised by the use of Wi-Fi is that wireless connections present an attractive mechanism for hackers to tap into the user's workstation to gain access to a corporate network.[5] A corporate network's protective measure (*e.g.*, firewalls and similar defensive software) could be by-passed under such circumstances because, when a user connects a workstation directly to the Internet, the workstation itself becomes the connection point, without the benefit of all the protections available to a corporate network. Every workstation connected directly to the Internet creates a separate opportunity for intrusion. Wi-Fi users can mitigate the risks of this intrusion by, for example, having the same or similar types of protections installed locally in the workstation that a corporate network provides. Regardless of the protective methods employed, members must consider the protection of customer information when determining whether to allow associated persons to use Wi-Fi or other types of new technology.

Remote Access

In addition to wireless technological advances that may raise concerns regarding the security of customer information, remote access to corporate networks through VPNs or other technology may raise similar concerns. As mentioned above, each year, more employees are taking advantage of alternative working arrangements by working from home and also working while traveling. While some employees may use wireless connections, others access corporate networks remotely through physical wire connections. Physical connections to corporate networks present similar concerns as Wi-Fi connections, although members can more easily address some of these concerns through the use of firewalls, routers, filters, and other means to guard against intrusion. Before permitting associated persons to access customer information remotely, members must implement appropriate measures to secure the customer information.[6]

Members' Obligations

As members update their technology and use new and different methods of communication, whether through the use of wireless technology or allowing employees to work remotely, they should consider whether these methods necessitate updates or changes in their policies and procedures. Each member should tailor its policies and procedures to address specifically the technology used by its associated persons with access to customer records and information. There can be no "one-size-fits-all" policy or procedure; however, members should consider the following, at a minimum:

- whether the member's existing policies and procedures adequately address the technology currently in use;
- whether the member has taken appropriate technological precautions to protect customer information;
- whether the member is providing adequate training to its employees regarding the use of available technology and the steps employees should take to ensure that customer records and information are kept confidential; and
- whether the member is conducting, or should conduct, periodic audits to detect potential vulnerabilities in its systems and to ensure that its systems are, in practice, protecting customer records and information from unauthorized access.

The use of new technologies can benefit members, employees, and customers; however, these new technologies can also present risks that members must consider and address appropriately. In some instances, the appropriate way to deal with these risks is not only through technological solutions, but may also involve changes to the member's training regimen and/or to the member's policies and procedures. Members should consider whether the adoption of new technologies would necessitate changes in its compliance policies and procedures or systems before implementation so that issues can be identified and addressed in a timely way and problems can be avoided. In this regard, members must understand their obligations under Regulation S-P and related SEC rules and interpretations, as well as the requirements to have policies and procedures and a supervisory scheme as mandated by NASD Rules 3010, 3012, and 3013.

Endnotes

1 As discussed in greater detail below, members must ensure that reasonable measures have been or will be implemented to protect customer information regarding the member's use of new technology before the member actually uses or allows its associated persons to use such technology.

2 Recent amendments to Rule 30 of Regulation S-P made in response to the Fair and Accurate Transactions Act of 2003 (FACT Act) govern the disposal of consumer report information. *See Disposal of Consumer Report Information*, Exchange Act Release No. 50781 (Dec. 2, 2004), 69 Fed. Reg. 71322 (Dec. 8, 2004).

3 A recent survey indicates that the number of telecommuters working from their home "almost every day" rose to over 12 million in 2004. *See Home-Based Work Force Grows 23% in Decade*, CBS Marketwatch (Oct. 20, 2004). In addition, the same survey showed that over 44 million employees performed some work at home in 2004, up approximately 3 million from 2003. *See More Bosses Getting Into the Telecommuting Biz*, USA Today, at B2 (Nov. 3, 2004). For the press release announcing the findings, *see www.telecommute.org/news/pr090204.htm*.

4 One significant concern that has driven recent regulations regarding the confidentiality and privacy of customer information is identity theft. *See* 69 Fed. Reg. at 71322 (noting that Section 216 of the FACT Act was "designed, in general, to protect a consumer against the risks associated with unauthorized access to information about the consumer contained in a consumer report, such as fraud and related crimes, including identity theft"). While some of the recent, high-profile cases of identity theft involve unauthorized access to electronic information, some recent reports indicate that the majority of identity theft cases are still committed with information obtained offline. *See generally ID Theft is Declining and Mostly Offline, New Study Finds*, Wall Street Journal, at D2 (Jan. 26, 2005) (discussing a 2005 study by the Better Business Bureau that found that approximately 68 percent of cases of identity fraud in 2004 relied on information acquired offline). Thus, members are reminded that their procedures should not focus solely on the use of electronic information, but should also address the proper use and destruction of paper documents (including, of course, consumer report information under the recent amendments to Regulation S-P) that could raise privacy concerns.

5 This is sometimes called a "back door."

6 Of course, members must also take reasonable measures to ensure that they have adequate procedures in place to address customer privacy concerns with regard to their current methods of communication (*e.g.*, procedures regarding the inclusion of confidential customer information in email messages).