The Asset Management Industry
SERVING INDIVIDUAL INVESTORS
INVESTMENT COMPANY INSTITUTE

MEMO# 20946

March 13, 2007

Federal Trade Commission Publishes Practical Guidance for Businesses on Safeguarding Personal Information.

[20946]

March 13, 2007

TO: PRIVACY ISSUES WORKING GROUP No. 2-07
SMALL FUNDS MEMBERS No. 22-07
TECHNOLOGY ADVISORY COMMITTEE No. 7-07
OPERATIONS MEMBERS No. 9-07
COMPLIANCE MEMBERS No. 12-07 RE: FEDERAL TRADE COMMISSION PUBLISHES PRACTICAL GUIDANCE FOR BUSINESSES ON SAFEGUARDING PERSONAL INFORMATION.

The Federal Trade Commission (FTC) has recently published *Protecting Personal Information, A Guide for Business* (the "Guide"), [1] which contains useful and practical information for businesses of all sizes to consider in establishing a data security plan. According to the Guide, a sound data security plan is built on the following five key principles:

1. Taking Stock – This principle involves a business knowing what personal information it has in its files and on its computers. The paper notes that, as part of the taking stock process, businesses may want to consider inventorying all of their computers, laptops, flash drives, home computers and other equipment to find out where sensitive data is stored.

2. Scaling Down – The Guide recommends that businesses keep only that sensitive personally identifying information that they need. If a business does not have a legitimate need for information, it should not collect it. If it does have a need, it should keep the

information only as long as necessary. The Guide recommends that businesses that are required to retain information to comply with the law develop a written records retention policy to identify what information must be kept, how to secure it, how long to keep it, and how to dispose of it securely when the business no longer needs it.

3. Locking It – The bulk of the Guide is spent discussing issues to consider relating to protecting sensitive personally identifying information. While appropriate security depends on the kind of information a business maintains and how it is stored, in developing a data security plan, businesses may want to consider four key elements: physical security, electronic security, employee training, and the security practices of contractors and service providers. The Guide contains advice relating to each of these elements, including the following:

- Assess the vulnerability of each of the business' electronic connections to commonly known or reasonably foreseeable attacks;
- Do not store sensitive consumer data on any computer with an Internet connection unless it is essential for the business;
- Assess whether sensitive information needs to be stored on a laptop. If not, delete it with a "wiping" program rather than with standard keyboard commands;
- Require employees to store laptops in a secure place;
- Consider allowing laptop users only to access sensitive information, but not to store the information on their laptops;
- If a laptop contains sensitive data, encrypt it and configure it so users cannot download any software or change security settings without approval from an IT specialist;
- Consider adding an "auto-destroy" function so that data on a computer that is reported stolen will be destroyed when the thief uses it to try to get on the Internet;
- Train employees to be mindful of security when they are on the road – they should never leave a laptop visible in a car, at a hotel luggage stand, or placed in checked luggage unless directed to by airport security. Additionally, if someone must leave a laptop in a car, it should be locked in a trunk and everyone who goes through airport security should keep an eye on their laptop as it goes on the belt; and
- With respect to contractors and services providers, the Guide recommends that, before outsourcing a function, the business investigate the company's data security practices and compare them to those of the business. The business also may want to insist that its service providers notify it of any security incidents they experience, even if such incidents do not lead to an actual compromise of the business' data.

4. Pitching It – The Guide recommends that business implement information disposal practices that are reasonable and appropriate to prevent unauthorized access to – or use of – personally identifying information. Such practices should be based on the sensitivity of the information, the costs and benefits of different disposal methods, and changes in technology. The Guide contains useful information regarding proper disposal and notes

that a business should make sure that employees who work from home following the business' procedures for disposing of sensitive documents, old computers, and portable storage devices.

5. Planning Ahead – According to the Guide, a business should consider preparing today for future breaches to reduce their impact on the business, its employees, and its customers. This can be accomplished by having a plan in place to respond to breaches, including procedures governing containing, investigating, and providing notice of the breach, as appropriate to consumers, law enforcement, customers, credit bureaus, and other businesses that may be impacted.

The Guide includes a list of additional websites and publications containing more information about securing sensitive data.

Tamara K. Salmon
Senior Associate Counsel

endnotes

[1] The Guide is available on the FTC's website at: http://www.ftc.gov/bcp/edu/pubs/business/privacy/bus69.pdf. *See also* the discussion of establishing an effective records management program in the Investment Company Institute's *Electronic Recordkeeping & Communications, Guidance for Investment Companies & Investment Advisers* (2006) (http://www.ici.org/pdf/ppr_06_elec_comm.pdf) ar 29-43, which provides advice consist with the FTC's Guide.