The Asset Management Industry
SERVING INDIVIDUAL INVESTORS
INVESTMENT COMPANY INSTITUTE

COMMENT LETTER

September 1, 2011

ICI Written Statement to ERISA Advisory Council on Privacy and Security Issues (pdf)

Statement of the Investment Company Institute ERISA Advisory Council Working Group on Privacy and Security Issues Affecting Employee Benefit Plans September 1, 2011 (Submitted August 30, 2011) The Investment Company Institute, the national association of U.S. investment companies,1 is pleased to submit this statement to the ERISA Advisory Council's Working Group on Privacy and Security Issues Affecting Employee Benefit Plans. Mutual funds and their investment advisers take investor security and privacy very seriously, and we are happy to share our members' insight. Our submission makes three key points: • The regulatory framework under which funds design their security programs works well because it is not prescriptive and provides funds broad discretion to tailor their security programs to their business and the needs of their investors. • Technology and the security threats that mutual funds face change rapidly, and regulators must provide flexibility to allow financial institutions to adapt their policies and procedures to changing conditions. • The fund industry has developed strong procedures and safeguards that rely on layered defenses, robust auditing, and a commitment from senior management. While fund companies' procedures share common elements, there is no "one-size-fits-all" approach that is best for every fund company and its investors. According to the latest Department of Labor data, there are over 650,000 defined contribution plans and over 48,000 defined benefit plans.2 These plans range from the very small to the very large, and 1 The Investment Company Institute is the national association of U.S. investment companies, including mutual funds, closed-end funds, exchange-traded funds (ETFs), and unit investment trusts (UITs). ICI seeks to encourage adherence to high ethical standards, promote public understanding, and otherwise advance the interests of funds, their shareholders, directors, and advisers. Members of ICI manage total assets of $13.3 trillion and serve over 90 million shareholders. 2 See Private Pension Plan Bulletin, Abstract of 2008 Form 5500 Annual Reports, Employee Benefits Security Administration (Dec. 2010), Table B8, available at http://www.dol.gov/ebsa/PDF/2008pensionplanbulletin.PDF. 2 there is a wide variety of ways that plans and their service providers store information and allow participants to access it. It is reasonable for plans to expect the financial institutions they engage to have security programs. There is no single set of procedures or guidelines, however, that will be appropriate for all financial institutions or plans. Therefore, there is no single checklist that plans should be expected or encouraged to use to evaluate service provider security programs. In this submission we first discuss in broad terms the regulatory framework under which mutual funds develop their policies and procedures for data privacy and security.3 Second, we describe how the mutual fund industry is meeting

the challenge of ensuring privacy and security of its customer data. Finally, we offer some comments on what lessons can be applied to retirement plans from the experience of fund companies. I. Regulatory Framework Section 501 of the Gramm-Leach-Bliley Act of 1999 directed the SEC and other agencies4 to establish appropriate standards for financial institutions relating to administrative, technical, and physical safeguards to protect customer records and information. The SEC implemented this directive in Regulation S-P.5 Regulation S-P requires that every investment company, investment adviser, broker, dealer, and transfer agent registered with the SEC adopt policies and procedures reasonably designed to meet three objectives. These procedures must: 3 Our submission focuses on how mutual funds protect customer data and not on various privacy notice regimes. There are a number of laws and regulations under the theme of "privacy" that require notices to be sent to customers and govern the extent to which financial institutions can use and share customer data for commercial purposes. For example, Regulation S- P (see note 5) requires a financial institution to provide its customers with a notice of its privacy policies and practices and prohibits the disclosure of nonpublic personal information about a consumer to nonaffiliated third parties unless the consumer is provided the opportunity to opt-out. Regulation S-AM, adopted by the SEC in 2009, restricts affiliates of mutual funds from using customer information to market products unless the customer is provided the ability to opt-out. See Regulation S-AM: Limitations on Affiliate Marketing; Final Rule, 74 Fed. Reg. 40398 (Aug. 11, 2009), available at http://sec.gov/rules/final/2009/34-60423.pdf. In our view, what is not needed here are more notices to participants. In fact, the Institute and others have testified about the need to streamline disclosures to participants. See Testimony of Lisa Hund Lattan on behalf of the Investment Company Institute before ERISA Advisory Council Working Group on Promoting Retirement Literacy and Security by Streamlining Disclosures to Participants and Beneficiaries (Sept. 15, 2009), available at http://ici.org/pdf/23804.pdf. Streamlining – not multiplying – notices to participants is consistent with President Obama's recent executive order on reducing regulatory burden. See Executive Order 13563, "Improving Regulation and Regulatory Review." (Jan. 18, 2011) (an agency should "tailor its regulations to impose the least burden on society, consistent with obtaining regulatory objectives, taking into account, among other things, and to the extent practicable, the costs of cumulative regulations"). 4 The Gramm-Leach-Bliley Act generally required coordinated efforts among the Office of the Comptroller of the Currency, Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Office of Thrift Supervision, Secretary of the Treasury, National Credit Union Administration, Federal Trade Commission, and the SEC, in consultation with state insurance regulators, on data privacy and security issues. 5 See Privacy of Consumer Financial Information (Regulation S–P); Final Rule, 65 Fed. Reg. 40334 (June 29, 2000), available at http://www.sec.gov/rules/final/34-42974.htm. 3 • Ensure the security and confidentiality of customer records and information; • Protect against any anticipated threats or hazards to the security or integrity of customer records and information; and • Protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer. In developing these standards, the SEC considered whether it should prescribe specific procedures that each entity subject to the rule must adopt, and sought comment on this point.6 The SEC believed, and the regulated community agreed, that it is more appropriate for each institution to tailor its policies and procedures to its own systems of information gathering and transfer and the needs of its customers. This approach has worked well. As described in more detail in Part II, based on the broad principles in Regulation S-P, fund companies have developed robust systems to protect customer records and prevent unauthorized access. In addition, since Regulation S-P was adopted, the technology underlying the data systems has changed rapidly, and so have fund procedures. For

example, when Regulation S-P was adopted in 2000, virtually no homes had Wi-Fi.7 By 2005, Wi-Fi was both in significant use and recognized as a potential threat.8 Because the requirements of S-P regulation apply regardless of changes in technology or media, SEC registrants had to address any security concerns arising in connection with the Wi-Fi technology to remain compliant with Regulation S-P.9 In 2008, the SEC proposed amendments to Regulation S-P to set forth more specific requirements for safeguarding information, responding to information security breaches, and broadening the scope of the information covered by Regulation S-P's safeguarding and disposal provisions.10 This proposed rule was patterned after rules adopted by the federal banking regulators after the enactment of the Gramm-Leach-Bliley Act. While expressing concerns with a number of 6 See Privacy of Consumer Financial Information (Regulation S-P); Proposed Rule, 65 Fed. Reg. 12354, 12365 (March 8, 2000), available at http://sec.gov/rules/proposed/34-42484.htm. 7 See "Growth of Wireless Internet Opens New Paths for Thieves," New York Times (March 19, 2005), available at http://www.nytimes.com/2005/03/19/technology/19wifi.html. 8 See id. 9 The National Association of Securities Dealers (now FINRA) issued a notice to its members reminding them of their obligations under Regulation S-P and suggesting they consider the risks that unsecured Wi-Fi poses to customer data security. See NASD, Notice to Members, "Safeguarding Confidential Customer Information" (July 2005), available at http://www.finra.org/web/groups/industry/@ip/@reg/@notice/documents/notices/p014772.pdf. 10 See Regulation S–P: Privacy of Consumer Financial Information and Safeguarding Personal Information; Proposed Rule, 63 Fed. Reg. 13692 (March 13, 2008), available at http://sec.gov/rules/proposed/2008/34-57427.pdf. 4 aspects of the proposal, the Institute generally supported this proposed rule, which would be even more rigorous than the SEC's current rule and would facilitate compliance by institutions subject to multiple regulators.11 The SEC has yet to adopt the amendments. But even as proposed, the amendments simply would enhance the framework under which mutual funds safeguard customer information. Importantly, the proposed rules would continue to provide flexibility to mutual funds to develop policies and procedures appropriate to the firm's size and complexity, nature and scope of activities and the sensitivity of personal information at issue. While Regulation S-P is the regulatory backbone for fund data security programs, there are other laws and regulations that govern fund procedures. For example, the Federal Trade Commission has "Red Flag" rules that require certain financial institutions to have and implement a written identity theft program.12 These rules apply to a mutual fund that offers accounts with check writing or debit card privileges.13 The Red Flag rules contain significant guidance to assist covered financial institutions in developing their identity theft program. The basic rule, however, is that the institution must develop policies and procedures that are designed to detect, prevent, and mitigate identity theft in connection with the opening or maintenance of an account. The rules make clear that the program must be appropriate to the size and complexity of the financial institution and the nature and scope of its activities. In addition, there are a number of state laws that apply to data security and privacy, a catalog of which is beyond the scope of this submission. These state laws present a particular challenge for mutual funds with investors in many states because they are not uniform and federal law does not preempt them.14 The multitude of these different laws necessitates regulatory flexibility at the federal level to facilitate the ability of financial institutions that operate in several jurisdictions to comply with all applicable laws. II. Mutual Fund Implementation of Security Policies and Procedures Within the broad discretion given to mutual funds and their advisers under federal requirements governing privacy, fund companies have developed robust and flexible policies and procedures to protect customer data. In fact, shareholder privacy and data security are a high priority for mutual funds. Shareholder and market perception of the reputation of a fund company and the adverse

consequences associated with a security breach or data loss are major drivers in achieving superior levels of protection for clients. 11 See Institute Comment Letter re: Proposed Amendments to Regulation S-P (May 2, 2008), available at http://www.sec.gov/comments/s7-06-08/s70608-22.pdf. 12 See Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003; Final Rule, 72 Fed. Reg. 63718 (Nov. 9, 2007), available at http://www.ftc.gov/os/fedreg/2007/november/071109redflags.pdf. 13 See FTC, The Red Flag Rule: Frequently Asked Questions, available at http://www.ftc.gov/bcp/edu/microsites/redflagsrule/faqs.shtm. 14 In addition, mutual funds with international operations must comply with rules in the countries in which they operate. 5 Like other financial service companies, mutual funds must confront a series of persistent and evolving attempts by bad actors to circumvent multiple security measures designed to protect shareholder non-public personal information. It is common for mutual funds to develop a layered process in their approach to security. This takes the form of managing both the physical access to facilities and the authentication and authorization process for access to computer systems to protect shareholder data. Among the risks that firms mitigate are operational risks that arise due to viruses, phishing, distributed denial of service ("DDOS") 15 attacks, website defacement and common fraud, each of which may harm a fund's customers and its reputation. Mutual fund firms view security as a process that depends on robust and current technology and well-trained employees. There is no "one-size-fits-all" approach to protecting information and privacy. Indeed, security experts warn against a one-size-fits-all approach to security because, if security is ever compromised, all institutions employing the same security method would be vulnerable, not just the institution originally compromised. Consequently, each organization will employ a variety of techniques appropriate to its size, business model, type of clients, vulnerabilities and its analysis of which combination of practices it believes will best protect shareholders and systems. Over time, and as technology and attacks evolve, mutual funds make adjustments to the different layers of security to ensure that shareholder information remains protected. Client service demands for timely, accurate, and meaningful access to account information change over time. As the use of electronic media expands, mutual fund companies continue to evolve their security and privacy strategies to meet the expansion. Not so many years ago, access to information and assets was done in person (e.g., at a branch of a fund or in the brokerage office) and during normal business hours, which later became supplemented by phone centers. As access became more automated and mobile through automated phone systems, automated teller machines and linked bank and brokerage accounts, face-to-face interaction quickly devolved. Today, clients may complete transactions online and wirelessly via mobile devices. As this technological and sociological evolution continues, mutual funds will continue to expand and leverage security and privacy practices to meet those changing demands for instantaneous access to information and assets, while protecting consumers' privacy and security interests. Mutual Fund Interaction with Customers Generally, mutual funds interact with shareholders in one of two methods: indirect or direct. Indirect activity is common today and occurs through a financial intermediary such as a broker-dealer, a bank, a financial advisor, or a retirement plan recordkeeper. With indirect activity, the shareholder generally interacts exclusively with the intermediary that interacts with the mutual fund on the shareholder's behalf. Direct activity occurs when a shareholder contacts the mutual fund over the internet, by phone, or through the mail to complete transactions (e.g., open accounts, place purchase and redemption orders, change account information). Whether the interaction is direct or indirect, 15 "Distributed denial-of-service" is an attempt by outside persons to flood a computer network with extraneous activity to the point where legitimate users are denied the ability to use the network. 6 mutual funds maintain sophisticated data security and

account privacy routines to protect information provided to them. The comments that follow speak to broad business practices that address both direct and indirect activities and are applicable to both taxable and non-taxable types of accounts. Staff Component An essential component of a robust security process is the commitment and support of senior management within an organization. The significant amount of resources mutual funds dedicate to security and education initiatives demonstrates the high priority given by senior management to securing the firm's shareholders' non-public personal information. One example of the security process funds may undertake is hiring highly specialized staff of certified computer security personnel in their IT departments. These individuals possess in-depth knowledge of access control, application development security, operations security, security architecture and design, and telecommunications and network security. In addition, these individuals maintain an expertise in the swiftly changing computer security environment through continuing education and training. Fund companies also spend a significant amount of time with staff outside the IT department on training and awareness in the responsible use of systems and in the protection of shareholder personal information, consistent with a firm's policies and procedures. As part of hiring processes, new employees may be screened through background investigations, including fingerprint checks. To provide financial protection should an event occur resulting in a financial loss, many employees are insured and bonded. Current staff members receive ongoing refresher training throughout their careers, which typically includes special training regarding fraud awareness, detection, and prevention. Due to the speed of technological changes and the inventiveness of those seeking unauthorized access to information, initial and ongoing employee training is a critical component in a fund's overall security and protection program. Layered Technical Defenses As mentioned above, to secure shareholder data and to prohibit unauthorized access and fraud, mutual funds employ layered technical defenses (LTDs) throughout their operations. LTDs are a combination of controls designed to create barriers against unauthorized access to information. The layers overlap with one another and include system tools, administrative procedures, and physical controls for the facility. In combination, LTDs provide a wrapper around data where unauthorized attempts to access information are met with multiple levels of protection. LTD tools in use include: • Firewalls that monitor data traffic for attempted unauthorized activity. • Antivirus software to combat malicious computer code entering a computer network. 7 • Intrusion detection monitoring that scans incoming activity for unauthorized access and for DDOS attacks. • Required shareholder validation routines for access to accounts. These routines are tailored for the type of system available to the shareholders. For internet access, shareholders may be required to complete a registration process to receive authorization for web access. After the registration, shareholders may be required to use credentials such as user identifiers and passwords, security questions, and user-chosen visuals to access information. For automated phone systems, shareholders may again be registered and then use specific credentials, which may include voice prints,16 to access the integrated phone system for data access. • Procedures to verify the identity of a phone caller such as security questions, key words or actual knowledge of recent activity. • System controls for employee access. Typically these controls consist of user identifiers and passwords as well as assigned user profiles which manage the extent to which an employee has the ability to access information based on the requirements of the job. Usually employee access is multilevel: the employee must have credentials to sign on to the company's computer network and then a second set of credentials to sign on to each of the recordkeeping systems needed to complete job requirements. • Procedures to monitor for activity that is inconsistent with the normal pattern in a shareholder's account. • Procedures to monitor for employee activity that does not match the expected actions necessary to complete a specific job function. • Procedures for regular updating of software to ensure the most

recent security protections provided by the software are in place on the computer network. • Procedures to confirm shareholder activity for account information changes and transactions, such as sending address changes to both the old and new addresses. Typically changes to address information also trigger an account hold period where any distribution activity must be done manually and include a signature guarantee medallion.17 16 Some firms keep previous recordings of shareholder conversations and can compare the recorded voice to the live voice to authenticate. 17 For additional information regarding signature guarantees, see the website of the Securities Transfer Association Inc. at http://www.stai.org/stamp.php. 8 • Facilities housing computer equipment and shareholder contact areas (such as areas for storing shareholder files and processing mail correspondence) are locked and protected with access restricted to only those authorized to work in those locations. Policies and Procedures Mutual funds maintain strong information security policies and procedures as part of their compliance programs. Such programs, which are required under the federal securities laws, require funds to have written policies and procedures to ensure compliance with the federal securities laws and rules (including Regulation S-P) and to regularly test them and make revisions necessary to address material weaknesses.18 The program must be overseen by the fund's Chief Compliance Officer, who reports to the fund's board, and the Chief Compliance Officer must annually provide the fund's board a written report detailing the testing efforts, any material weaknesses, and any changes to the policies and procedures.19 This framework is a critical component of a fund's overall compliance with security and privacy requirements. While these policies and procedures operate to satisfy specific regulatory requirements, they often cover a broader array of areas, including: • Information security • Privacy • Information and records management • Computer usage • Shareholder communication and information access • Employee policies regarding the use of computer and mobile devices • Employee code of ethics regarding overall conduct of the employee (including conduct related to shareholder privacy and data security)20 • Use of social media In addition, mutual funds have policies and procedures for business continuity planning (BCP). BCP covers a broad range of activities, including the need to maintain data security in emergency situations when normal operations are interrupted. During a BCP event, the same levels of logical and physical controls must be employed to ensure that information is protected and shareholder privacy is maintained just as if normal operations were in effect. Moreover, additional protections may be warranted to service customers who have lost access to account information or their normal means of communications with the fund (e.g., after events like hurricane Katrina). 18 See Rule 38a-1 of the Investment Company Act, 17 C.F.R. § 270.38a-1. 19 See id. 20 Typically this policy requires an annual certification of the employee attesting to adherence to those rules. 9 Audits and Testing Mutual funds maintain a robust regime of auditing and testing of security and privacy programs as a key component in providing safe coverage for shareholder information. Audits and tests are completed regularly (some on a schedule, some ad hoc) throughout the year. Results are distributed to appropriate management, with necessary corrective actions initiated. Such audit and testing of security and privacy programs will often include: • Engaging third party security auditors to test the cohesiveness of the security programs. • Utilizing internal audit and compliance programs to monitor and test both security and privacy procedures. • Establishing procedures to test new computer software before that software is placed into everyday use. • Conducting facility audits, such as "clean desk" audits, in which risk staff will visit work areas looking for shareholder information that has not been secured in locked files or, if no longer needed, shredded into locked shredding bins. Like all financial institutions, mutual funds commonly use vendors. The vendors may provide services, facilities, hardware (such as computers and information storage devices) and software, or any combination of these. Where a vendor is contracted to manage or store information,

mutual funds typically complete a vigorous due diligence evaluation to assess the level of security protection in use by the vendor. This evaluation may include site visits, extensive questionnaires, and reviews of third party audits such as SSAE No. 16 (formerly SAS No. 70).21 Mutual funds may conduct these evaluations both at the inception of the relationship and on a regular basis (typically annually) during the term of the contract. Plan sponsors can expect their plan recordkeeper to perform similar monitoring of vendors with access to participants' non-public personal information. III. Lessons for Retirement Plans There are important lessons that the Council can take from the experience of mutual funds in addressing security challenges: Participants holding their accounts at a mutual fund complex benefit from the protections afforded to them by Regulation S-P and the federal securities laws. Mutual funds are prized by retirement plans because they operate under a regulatory framework that holds advisers and fund 21 For more information on SSAE No. 16 and its transition from SAS No. 70, see the American Institute of Certified Public Accountants website at: http://www.aicpa.org/News/FeaturedNews/Pages/SASNo70Transformed%E2%80%93ChangesAheadforStandardonServ iceOrganizations.aspx. 10 boards to fiduciary standards, strictly regulates conflicts of interest, and imposes disclosure rules with the needs of ordinary investors in mind. Additionally, plan sponsors and participants holding their accounts at a mutual fund complex gain access to the robust security procedures fund companies have developed.22 Moreover, when a plan sponsor uses a mutual fund company to provide defined contribution plan recordkeeping and similar services, the fund company can often apply its data security technology and procedures in its recordkeeping systems. Rules that provide broad guidelines and allow institutions to adapt to changing conditions work best. Any strict rules or checklists referencing today's technology will become hopelessly out of date quickly. Further, while "safe harbors" can work well in other regulatory contexts, they do not work well where policies and procedures must be adapted over time to particular systems of information gathering and the needs of participants or investors. There is no one-size-fits-all approach to security. Neither the Council nor DOL should conclude that every plan from the smallest to the largest plan needs the kind of procedures that mutual funds have developed or that all mutual funds should employ the same security and privacy safeguards. The hundreds of thousands of retirement plans and the companies that sponsor them come in all shapes and sizes. No small business owner will sponsor a plan if it requires becoming an expert in data security. Plan sponsors should be able to rely on their service providers to use commercially reasonable methods to protect customer data. * * * * Thank you for inviting the Institute to share its views and its members' experience on how to best protect those saving for retirement. We applaud the Council for looking at this topic and look forward to the Council's report to the Department of Labor. 22 As a technical matter, Regulation S-P only protects information of individuals and not institutional investors like pension plans. See SEC Staff Responses to Questions About Regulation S-P, Question 4 (updated Jan. 23 2003), available at http://www.sec.gov/divisions/investment/guidance/regs2qa.htm. As a practical matter, however, funds apply their policies and procedures to protect all customer data in their possession, whether the account is held by an individual or an institution. In many cases, the plan's account at the fund is held by a retirement plan recordkeeper and not the plan itself so the fund company may not have individual participant data. Instead, the plan's recordkeeper may maintain that information.

should not be considered a substitute for, legal advice.