# The Two Faces of Identity Theft

## Of Data and Dollars

Originally Published in January 2006

# The Two Faces of Identity Theft

# Introduction and Executive Summary

Identity theft — the impersonation of an individual through unauthorized use of personal information about that individual — is reportedly one of the fastest growing crimes in the country.[1] It is also an issue of growing interest and concern to the public, press, legislators, and regulators. Results of a recent survey suggest that Americans now rank identity theft nearly even with terrorism and the state of the economy among their primary concerns.[2] Numerous recent media stories have reported corporate and governmental losses of tens of millions of consumer records, and lawmakers and regulators have been focusing increased attention on the issue. Even plaintiffs' lawyers have become involved, with the filing of lawsuits that seek to hold large institutions responsible, under various legal theories, for loss of customer information and for financial losses incurred by customers as a result of identity theft.

The broad concept of "identity theft" encompasses two distinct sets of concerns for fund complexes:

- The first set of concerns relates to the *loss or unauthorized disclosure of personal information entrusted to the fund complex*. If personal information on shareholders (or employees) held by a fund complex is lost or misappropriated, identity thieves may be in a position to obtain and misuse such information — to abscond with assets from shareholder (or employee) accounts at the fund complex itself, to abscond with assets from financial accounts held by those shareholders (or employees) at *other* institutions, to open illegitimate lines of credit in the names of those shareholders (or employees), or otherwise to adversely impact their financial health.[3]

- The second set of concerns relates to the *misappropriation of assets held by the fund complex*. If an identity thief is able to obtain — from the fund complex, directly from a shareholder, or elsewhere — sufficient personal information on the shareholder, the thief may be in a position to "hijack" the shareholder's accounts at the fund complex and abscond with shareholder assets.

In short, the first set of concerns is primarily directed at preventing identity theft from occurring in the first instance, whereas the second is generally aimed at avoiding the consequences of identity theft that has already occurred.

In recognition of the financial, legal, and reputational impacts that identity theft may have on fund complexes, ICI Mutual Insurance Company, a Risk Retention Group ("ICI Mutual" or the "Company") has conducted this study ("Study"). Written specifically for senior management and for legal and compliance personnel, this Study is designed to assist fund complexes in assessing identity theft risks, and in developing and implementing strategies to manage and reduce these risks. This Study explores techniques used by fund complexes and other organizations in preventing the loss of personal information that may give rise to identity theft. Moreover, recognizing that the ability of fund complexes to prevent identity theft is often limited, this Study also considers techniques that may be used to safeguard assets held by fund complexes against misappropriation by identity thieves.

This Study supplements information provided in *Computer Security Lite,* the Company's 2003 study on managing computer security risks.[4] While this earlier work recognized the close relationship between computer security and data security, it was not intended to address specific issues regarding identity theft. Over the past three years, however, the increased incidence and severity of data losses — especially in various parts of the financial services industry — have highlighted the

importance of financial institutions focusing greater attention on identity theft and related data security issues.

The observations in this Study are derived from ICI Mutual's detailed interviews with selected fund complexes, from discussions with outside data security experts, and from ICI Mutual's examination of publicly available information on identity theft issues. This Study is not intended to and does *not* recommend any single structure or set of "best practices" to be used by fund groups in managing identity theft risks. Given the diversity of both the investment management industry and threats to data security, it is not advisable or practical to seek a "one size fits all" standard in this area.

This Study is divided into two sections:

- The first section provides an overview of identity theft, focusing on how fund groups may be affected either by a failure to safeguard personal information or by a failure to safeguard assets of individuals whose personal information has already been compromised. This section also reviews common means used by perpetrators to illicitly obtain personal information about individuals (either from fund complexes or from other sources, including the affected individuals themselves).

- The second section describes strategies and techniques that may be helpful in detecting and managing risks associated with identity theft. More specifically, it sets forth a number of questions that fund groups may wish to consider in designing their own programs for protecting personal information and shareholder assets against the risks of identity theft.

# Overview

With recent, highly publicized losses by large institutions of personal information about millions of individuals, the issue of identity theft — the impersonation of an individual through unauthorized use of personal information about that individual — has achieved considerable prominence. Increasingly, the public, the press, legislators, and regulators have expressed varying degrees of outrage, concern, and nervousness about the issue. But what does identity theft mean for fund complexes?

Shareholders (and frequently, employees) have entrusted fund complexes with their personal information, including both identifying information (such as Social Security numbers and dates of birth) and financial information (such as account numbers). Shareholders, of course, have also entrusted fund complexes with their assets. Fund complexes are expected to safeguard both. Identity theft places both at risk.

### Two Faces of Identity Theft

- Loss of personal information, resulting in identity theft
- Loss of assets as a result of identity theft

## Consequences

As discussed in the introduction to this Study, identity theft encompasses concerns over both (1) loss of personal information about individuals and (2) misappropriation of the financial assets of those individuals. In considering the consequences of identity theft, it is helpful to focus separately on the two areas.

### LOSS OF PERSONAL INFORMATION

Fund complexes may collect and maintain many different types of personal information about individuals, including personal identifying information about shareholders, employees, and even prospective employees, financial information about shareholders and employees, and medical information on employees.[5] Identity thieves who gain access to such information may seek to misuse it in order to abscond with shareholder and employee assets (whether held by the fund complex itself or in accounts at *other* financial institutions), to open illegitimate lines of credit, or otherwise to adversely affect the financial health of the shareholders and employees. The regulatory, legal, and/or reputational repercussions for a fund complex that loses or discloses without authorization such personal information can be significant, even if the loss or unauthorized disclosure ultimately has no direct financial impact on the affected individuals.[6]

Particularly in industries, such as the mutual fund industry, where consumer trust is central to successful operations, loss or unauthorized disclosure of personal information can result in significant reputational harm and lost business opportunities.[7] Costly public relations campaigns may also be required to shore up customer confidence.[8] Indeed, in the wake of recent losses of large amounts of personal information by large institutions, several surveys have suggested that customers may be moving away from providers responsible for the loss of personal information,[9] and that customers may generally be more reluctant to engage in electronic transactions.[10]

Loss or unauthorized disclosure of personal information by institutions may also carry regulatory and legal consequences. There are a patchwork of laws and regulations that may be implicated as a result of loss or unauthorized disclosure of personal information. While a detailed discussion of how these laws and regulations may apply to the fund industry is outside the scope of this Study, it is important to recognize that lapses in the safeguarding of personal information may implicate

numerous data security and privacy-oriented laws on both the federal and state level,[11] as well as federal and state regulations,[12] and even foreign laws.[13] Notably, a California law generally requires companies that believe that there has been a breach of security of a database containing unencrypted information to notify any affected or potentially affected individuals.[14] Many data security experts credit this law (and other similar state laws[15]) with driving many of the recent disclosures by institutions of database breaches.[16] Moreover, based on recent events — and on public insistence on greater protections[17] — it appears that new or tougher data protection laws may be enacted.[18]

Recent lapses in database security have also spawned a number of lawsuits by private litigants. For example, class action lawsuits have been filed in federal court against a large business provider of identification and credential verification services, alleging that the company's loss of information about consumers amounted to violations of consumers' rights under federal and state credit reporting laws and their rights to privacy.[19] These lawsuits are *not* predicated on allegations of actual identity theft resulting from the database breach;[20] indeed, no instance of identity theft has yet been traced to the companies' loss of consumer information. Rather, these lawsuits focus on the concern that identity theft *may* have occurred.[21]

### LOSS OF DOLLARS

The loss or unauthorized disclosure of personal information about a fund complex's shareholders creates the opportunity for the misappropriation of shareholder assets held by the fund complex. If an identity thief is able to obtain sufficient personal information on shareholders, the thief may be in a position to "hijack" the shareholder's accounts at the fund complex, and abscond with shareholder assets through unauthorized written, telephonic, or on-line instructions.

Depending upon the particular circumstances involved, a fund complex may have no actual legal liability or even apparent responsibility for shareholder losses resulting from identity theft, particularly where the fund complex has not been implicated in the loss or disclosure of relevant shareholder personal information. Nevertheless, there are those who would seek to make the fund complex a guarantor for any shareholder losses. Particularly in the area of on-line transactions, enterprising lawyers have been developing novel theories under which they seek to hold financial institutions responsible for financial losses sustained by individuals as a result of identity theft. For example, in one lawsuit, a bank customer who sustained an on-line fraud loss as a result of his own disclosure of personal information is seeking to hold the bank responsible, not by reason of any claimed deficiency in the bank's own practices and procedures, but rather on the theory that the bank had been negligent in failing to notify its customers of "specific security procedures they [i.e., the customers] needed to undertake in order to prevent online banking fraud."[22]

Of course, regardless of who bears ultimate responsibility for any financial loss, if shareholder assets are misappropriated as a result of identity theft, the result will almost certainly be a disruption in the relationship between a fund complex and the affected shareholder(s). To the extent such incidents become public, there may also be a loss of shareholder confidence in the ability of the fund complex to safeguard shareholder assets, and other adverse reputational impacts.

## Means of Loss

Because the two faces of identity theft are either directly or indirectly concerned with losses of information, it is helpful to consider how such losses happen. While sensitive personal information may be lost by fund

complexes (or their affiliates and service providers), it may also be lost by the affected individuals themselves or by other third parties. Regardless of the party responsible, however, there are two broad avenues by which such losses occur — "traditional" and electronic. By either avenue, the identity thief who obtains the information may seek to misappropriate the assets of the affected individuals or to use the information for other illicit purposes.

## TRADITIONAL LOSSES OF PERSONAL INFORMATION

Even as media and public attention focuses on electronic losses of personal information, "low-tech" losses remain prevalent.[23] Identity thieves — who come in various guises, ranging from the stranger working in anonymity over the Internet to a disaffected family member of a victim with ready access to the victim's account statements and passwords — utilize a number of such "low-tech" methods. These include "dumpster diving" (i.e., looking through an individual's or an entity's trash), theft of personal papers, and direct solicitation of institutions and individuals.

As regards direct solicitation, it is axiomatic among data security experts that people, and not computer systems, present the biggest potential threat to data security.[24] In direct solicitation (i.e., "social engineering") attacks (which, as described in the next section, may also be conducted electronically), identity thieves seek to induce or trick *customers* into providing their passwords and other sensitive information, or, alternatively, seek to induce or trick an organization's *employees* into providing customer information or into permitting access to the organization's facilities. Social engineering attacks, which studies have shown to be surprisingly successful, exploit the carelessness or naïveté of customers or employees, or simply capitalize on their desire to be helpful.[25]

Low-tech loss of electronic hardware may also lead to losses of personal information. Thus, for example, theft of physical property (such as laptops storing sensitive information) may permit an identity thief to access personal information stored electronically. Similarly, ordinary disposal of hard drives or other computer equipment by an individual or organization may permit an identity thief to "dumpster dive" and thereby obtain sensitive electronic information.

## ELECTRONIC LOSSES OF PERSONAL INFORMATION

Despite ongoing concerns over "low-tech" loss of personal information, the emergence of identity theft as a serious risk has been driven largely by the rise of the Internet and by the rapid increase in electronic collection, storage, and transmittal by institutions of personal information on a multitude of individuals. In particular, identity theft can frequently be traced back to losses of personal information resulting from (1) breaches (or losses) of databases maintained by institutions, (2) software programs (known as "spyware") used by perpetrators to collect personal information directly from the personal computers of individuals, and (3) electronic subterfuge used by perpetrators to induce individuals into voluntarily giving up personal informa-

### Recent Large Data Breaches

*CardSystems* — Exposure of credit card information (including security codes) about 40,000,000 customers

*Bank of America* — Loss of backup tapes containing account information about 1,200,000 customers

*DSW Shoe Warehouse* — Theft of credit card information about 1,400,000 customers

*Time Warner* — Loss by data storage firm of personal information about 600,000 current and former employees

*Lexis-Nexis*— Theft of identification codes and passwords of 310,000 customers

tion (for example, by "phishing" or by a new variant, called "pharming").

Over the past eighteen months, the media have reported regularly on incidents in which databases of customer or employee information maintained by institutions have been breached or lost. In the aggregate, personal information on tens of millions of individuals has been actually or potentially exposed to public view.[26]

"Spyware" programs — a form of malicious software — are used by perpetrators to collect personal information directly from the personal computers of individuals. Customers unknowingly download and install a "spyware" program on their personal computers by clicking on an e-mail attachment or a website. Once the program installs itself on a customer's computer, the program then secretly gathers and sends to the perpetrator information (such as a Social Security number or password) that the customer may type on his computer keyboard during the course of otherwise legitimate electronic transactions, or that the customer may store on his or her computer.

## Electronic Losses

- Loss resulting from database breaches
- Loss through spyware programs
- Loss through phishing and pharming

Electronic subterfuge may also be used by perpetrators to deceive individuals into voluntarily giving up personal information, with the perpetrators then using this information to perform transactions in a customer's account, or to open up additional accounts. In a typical "phishing" scheme, for example, perpetrators arrange for blanket distribution of e-mails that purport to be sent by legitimate financial institutions, but that link instead to fraudulent websites that appear identical to the real websites of the financial institutions. Respondents to phishing e-mails are typically asked to enter personal information on the fraudulent websites, thereby surrendering this information to identity thieves.

Recent studies have estimated that the number of phishing e-mails rose from 337,000 in January 2004 to 4.5 million in November 2004,[27] and that, in a single year, nearly two million people lost $2.4 billion through phishing schemes.[28] Some observers have estimated that the response rate to phishing e-mails is as high as five percent.[29] As phishing scams have matured, fraudsters have begun to target smaller organizations, which may be less prepared to combat the threat.[30] This explosive growth, combined with a relatively high response, underscores the seriousness of this issue.

"Pharming" is another relatively new and growing threat. One expert has stated, "Phishing is to pharming what a guy with a rod and a reel is to a Russian trawler."[31] Unlike phishing attacks, which rely on trickery to obtain personal information, pharming attacks do not. In a pharming attack, an Internet user attempting to access a legitimate website will, without his or her knowledge, be redirected to a fraudulent website that appears identical to the legitimate website. One means of effecting this type of attack is by corrupting the DNS (domain name system) servers that are used to translate domain names (such as www.whitehouse.gov) into their corresponding numeric IP address (e.g., 127.0.0.1).[32] In March 2005, over a thousand Internet domains were reportedly redirected to fraudulent websites.[33] Like "phishing" schemes, "pharming" permits identity thieves to gain personal information about customers without their knowledge or consent.

# Strategies and Techniques for Addressing Identity Theft

Strategies and techniques used by fund groups to manage risks associated with identity theft are necessarily influenced by a number of factors, including the size of the fund group, the extent of its reliance on outside vendors and service providers, and the nature of the fund group's computer systems, applications, and interactions with shareholders and other third parties. In developing programs for addressing identity theft issues, fund groups may wish to consider, among other things, the questions set forth below regarding such strategies and techniques. While most of these strategies and techniques may have some utility in preventing either a loss of data or a loss of dollars, some techniques may be more suited to one or the other. For example, the encryption of databases is primarily aimed at averting a loss of information (although encryption — e.g., of passwords or Internet transmissions — may also prove useful in protecting against misappropriation of shareholder assets).

## Data Security Programs

*How does your complex decide what categories of information require protection? Does your complex have specific policies and procedures regarding data security? Does your complex maintain a strong computer security risk management program?*

As discussed earlier in this Study, prevention of "identity theft" encompasses efforts to safeguard personal information entrusted to fund complexes. In establishing data security programs, many fund complexes have found it useful to establish relative priorities for protecting sensitive information. Fund complexes may consider a variety of factors in making such assessments, including: (1) identification of the categories of information considered valuable to the organization, (2) ranking of the relative importance of protecting each of these categories of information, (3) identification of the specific types of threats to each of these categories (e.g., computer security breaches, "social engineering" attacks), and (4) evaluation of the vulnerability of each such category of information to these various threats.

Fund groups may find it helpful to establish data security programs that set forth the organizations' general policies on the protection of personal information and other sensitive data.[34] Such programs may also provide specific guidelines on the storage and use of personal information.

Limiting access to information can assist in reducing the risk of identity theft. Fund groups generally implement various authentication procedures designed to ascertain the identity of persons who seek to use the complexes' computer systems. Some of these authentication procedures are discussed in greater detail on page 12. Moreover, some fund complexes find it useful to impose strict authorization procedures that limit a particular user's ability to change or even read certain files and documents (such as those not needed by the user to do his or her job.)

In addition, some fund groups have implemented comprehensive auditing procedures with respect to access to information. These procedures permit fund groups to create audit trails that detail who accessed certain information, or who tried, but failed, to access such information. Such auditing procedures may be helpful in preventing or limiting the extent of any loss of

information, and in quickly detecting any losses that do occur.

As with compliance programs generally, data security programs often detail how and by whom the programs will be implemented and maintained. Such programs also frequently specify how and by whom data security incidents will be addressed, as well as how and by what criteria data security incidents will be escalated to increasingly senior levels of the organization.

Fund complexes have recognized the importance of retaining knowledgeable and capable individuals to implement data security programs. While the day-to-day responsibility for implementation of such programs often falls to the IT departments of fund complexes, over the past several years, some companies have established chief privacy officer ("CPO") or chief information security officer ("CISO") positions to implement, oversee, and manage data security programs. Moreover, addressing identity theft issues typically requires the participation and involvement of a number of other groups within an organization, as well as others outside the organization. For example, the involvement of senior management and other appropriate personnel (including the IT department) is invaluable in establishing goals for a data security program and the levels of resources to be devoted to the effort. Other internal groups (such as customer service representatives) may also have a critical role in preventing, or at least not contributing to, loss of personal information. Indeed, every person in an organization may have a role in helping the organization avoid the loss of personal information

The sheer amount of information stored and processed in electronic form highlights the importance of implementing strong and effective programs for managing data security risks. ICI Mutual's 2003 computer security study explored techniques and practices that fund complexes and other organizations have found useful in enhancing computer security. In the time since that study was completed, fund complexes report that they have continued to apply — and refine — those techniques and practices.

## Encryption

*Does your complex encrypt data reflecting personal information? If so, what types of data are encrypted? How does your complex determine whether to encrypt data and which types of data should be encrypted?*

Encryption refers to the process of scrambling information so that it cannot be understood without a password or other means of deciphering the information. Depending on the type of information to be encrypted, fund complexes have a number of encryption algorithms available to protect information.[35]

In determining whether to encrypt particular types of data, fund complexes have considered a number of factors. Because use of encryption may adversely affect network performance and user functionality, encryption may impose costs on an organization in the form of (1) increased hardware costs to offset any performance penalty and (2) lost productivity. Moreover, the use of different encryption standards by different organizations (such as vendors and affiliates) may hamper the ability of fund complexes to communicate with third parties. Notwithstanding these potential adverse impacts, encryption can significantly increase an organization's overall data security by inserting another layer of protection over sensitive information.

**Ameritrade**

The data in a lost backup tape were compressed, but do not appear to have been encrypted.

*Customers Affected: 200,000*

Certain types of data are frequently encrypted by financial institutions, including many fund complexes. For example, fund complexes commonly encrypt passwords used by shareholders, insiders, and other authorized users to gain access to network systems. Moreover, transactions effected over the Internet typically are secured by 128-bit Secure Sockets Layer ("SSL") encryption. Fund complexes also often use encryption to protect remote access connections to computer networks by employees or by other authorized users, including consultants and service providers.

The use of encryption appears to be less common in other contexts. For example, it appears that many fund complexes are not now encrypting information in electronic databases generally or in other files.[36] Similarly, the use of encryption for information that is sent off-site for backup or storage does not appear to be widespread.[37] In addition, while some fund complexes seek to encrypt information stored on laptop computers, it is not clear that this is a common practice.

As organizations increasingly share sensitive information with third parties, including affiliates, service providers, and shareholders, a number of organizations have reevaluated the issue of encryption. In particular, some companies, including some financial institutions, have determined to encrypt more of their data, particularly data that are being sent off-site for backup and storage.[38] While few fund complexes appear to have yet moved toward greater use of encryption, many report that they are considering it.

### Time Warner

Personal information about current and former employees that was not encrypted disappeared while in the custody of a data storage firm.

*Employees Affected: 600,000*

Fund complexes may also wish to consider any relevant legal issues regarding data encryption. Under California law, for example, the shareholder notification requirement applicable to certain types of data loss does not apply if the lost data were encrypted.[39]

## Enhanced Authentication

*What types of measures does your complex use to authenticate the identity of shareholders, employees, business partners, or other third parties who may have access to sensitive information? Has your complex considered the use of additional authentication measures? If so, what additional measures? Has your complex considered whether to establish means for shareholders to authenticate the identity of your complex?*

Effective data security programs seek, among other things, to ensure that access to sensitive data is limited to users whose identity has been properly authenticated. Authentication describes the process for confirming the identity of a user seeking access to such data; that user, once authenticated, is then permitted access to data to which he or she is authorized. While frequently discussed in the context of on-line communications, the concept of "authentication" also encompasses non-electronic measures for verifying identities, such as use of signature guarantees (for written documents) and recitation of personal identification numbers (for telephonic transactions).

The authentication process may involve one or more factors, depending on what is required to establish the identity of a user. In "single-factor" authentication, the identity of a user is tested entirely on the basis of something the user *knows*, such as a password, that is unique to that user. While providing protection, the use of single-factor authentication does not guarantee complete security. Indeed, recent incidents of identity

theft underscore the pitfalls of relying solely on passwords or other single-factor techniques.

In recognition of these pitfalls, some companies and vendors are using stronger versions of single-factor authentication. While still relying on what a user *knows*, these stronger single-factor authentication measures require, in essence, *more* knowledge from the user. For example, these measures may authenticate a user by asking a series of questions (such as the name of the user's mortgage company, the monthly mortgage payment, information about other consumer loans, and similar information) and then comparing the answers to information on file with credit reporting agencies.[40] These measures thus strengthen security by requiring more extensive proof before authenticating the person's identity.[41]

## Authentication Factors

### WHAT YOU KNOW

- User ID
- Passwords

### WHAT YOU HAVE

- Hardware token
- Smart card

### WHAT YOU ARE

- Fingerprints
- Retinal scans

Some financial institutions enhance their single-factor authentication procedures by seeking to verify a customer's identity using a different channel of communication ("out-of-band" authentication). Under this technique, a customer using a website to conduct a transaction may then be contacted by the financial institution by phone or e-mail to verify the customer's intention to engage in the transaction.[42]

The addition of a second authentication factor further enhances security. "Two-factor" authentication tests not only what the user *knows*, but also what the user *has*. Under two-factor authentication, users must typically not only establish their identity through use of a password (what the user *knows*), but must confirm their identity through use of an object, such as a hardware identification token, smart card, or USB dongle (what the user *has*). Some authentication systems also add a third factor — what the user *is*. Examples of a third authentication factor include biometrics (for example, fingerprints or retinal patterns). For the sake of simplicity, this Study uses the term "two-factor" authentication to refer to the use of a combination of (1) a password (or other knowledge), and (2) any additional authentication factor (whether it pertains to what a user has or what a user is).

A number of fund complexes require *employees* to use two-factor authentication in accessing the complexes' computer systems and may also require two-factor authentication of vendors. However, few if any fund complexes appear to require two-factor authentication of shareholders at this time. While some fund complexes have considered use of two-factor shareholder authentication, they have deferred implementation, citing, among other things, costs of implementation and concerns over customer acceptance.

Even in the banking world, where many top banks apparently offer the use of two-factor authentication to large corporate clients, it appears less common to offer such authentication to small business clients or individual customers.[43] It is noteworthy, however, that Bank of America has recently announced plans to expand use of two-factor authentication (specifically, the use of an external password-generating token device that generates a random log-in number).[44] Some other organizations,

including AOL and E-Trade, have also reportedly begun to offer two-factor authentication to their customers.[45]

Enhanced authentication measures by financial institutions are likely to become more prevalent in the coming years as a result of technological advances and/or regulatory and public pressure.[46] A nationally known computer security consulting firm interviewed for this Study reports that it is now receiving numerous inquiries from financial institutions (including some fund complexes) about the use of two-factor authentication for retail customers, whereas it had received virtually no inquiries as recently as a year ago. Indeed, two impediments to widespread use of two-factor authentication — cost and public resistance — are likely to become less significant in coming years, as technological advances make such authentication devices cheaper and as growing awareness of the risks of identity theft persuades the public to more willingly accept some inconvenience in return for greater security. Enhanced authentication is not foolproof,[47] but it does appear to provide a significant increase in security.[48]

Authentication can be a two-way process. Not only is there increased interest on the part of organizations in authenticating *users'* identities, but, given the rise in phishing and pharming incidents, there is also increased interest on the part of users in authenticating *organizations'* identities. Because online services provided by financial institutions are conducted on secure Internet connections (and fraudulent websites tend not to use secure connections), users may seek to distinguish between legitimate and fraudulent websites by checking to see if the connection is secure (e.g., the website's address will begin with "https" rather than "http"). Some Internet browsers, such as Mozilla Firefox, provide a visual indication that a user is on a secure site.

Use of digital certificates provides another means by which customers and websites may mutually authenticate the other's identity, thereby reducing (although not eliminating) the website's vulnerability to phishing or pharming attacks.[49] Some companies are also exploring other means of authenticating their identities to their customers. For example, Bank of America has begun to offer a service that allows online customers to verify that they are logged into the bank's true website by displaying an image and phrase that the customer has previously provided to the bank.[50]

## Measures Taken by Service Providers, Affiliates, and Other Third Parties

*What steps does your complex take to protect information that is shared with or sent to outside service providers, affiliates, and other third parties? To what extent do data security considerations factor into the decision to enter into business relationships with service providers, affiliates, and other third parties?*

Fund complexes routinely share information with, or provide network access to, various third parties, including service providers, affiliates, and even government agencies. This widespread sharing of information provides more avenues through which sensitive information may be lost, stolen, or otherwise misused. Such sharing also surrenders some degree of control over that information to third parties. As a result, fund complexes typically consider not only their own measures to protect data security, but also the measures taken by those third parties.

After assessing the data security risks presented by third parties, fund complexes have employed various tech-

**Bank of America**

Backup tapes containing federal workers' customer and account information, including credit card data, were lost during shipment to a backup data center.

*Customers Affected: 1,200,000*

niques to limit such risks. For example, some fund complexes actively seek to limit the information made available to third parties to the absolute minimum required for the third parties to fulfill their responsibilities. Other measures, such as encryption of data and the use of enhanced authentication techniques, are discussed in more detail earlier in this section.

Fund groups report that it has also become a more common practice to audit data security practices and procedures of various service providers and business partners, so that fund groups may satisfy themselves as to the adequacy of the security being provided.[51] Some fund complexes report that data security risks have become an increasingly important consideration in decisions regarding entry into new business relationships. In some circumstances, fund complexes are also considering whether an onsite review of data security measures used by existing or prospective providers and business partners would be appropriate.

In addressing data security issues in their contract negotiations with service provider and business partners, many fund complexes focus attention on prevention of data losses (e.g., by including contractual requirements that a business partner maintain systems to prevent data losses). While recognizing that the loss of sensitive information may inflict irreversible harm, fund complexes nevertheless typically seek indemnification provisions covering damages resulting from a business partner's failure to maintain adequate data safeguards.

## Physical Security

*What physical security measures are taken by your complex to ensure the physical security of data or of the systems or facilities housing such data?*

Many means of protecting data are intended to prevent unauthorized electronic access to computer systems. However, computer systems are also vulnerable to illicit physical access. Of course, information existing in paper format also requires physical protection.

### San Jose Medical Group

Patient records and Social Security numbers were lost when computer equipment was stolen.

*Customers Affected: 185,000*

One goal of physical security measures is to ensure that a fund complex knows the identity of individuals who are on the premises of the complex. Through the use of radio frequency identification ("RFID") cards, security cameras, and other technologies, some organizations even have the ability to track where individuals are in the building and, where deemed appropriate, to limit the access of users to certain parts of the premises.[52] A company may require an individual to produce a picture ID card or to undergo a fingerprint or retinal scan before entering certain facilities, such as those housing the company's network servers or sensitive paper files.

### SAIC

Computer equipment containing information about former and current employees was stolen.

*Employees Affected: 45,000*

Most computer equipment stored in a complex's physical plant — such as network servers and, to a lesser extent, desktop computers — is protected by some degree of physical security. By contrast, laptop computers and other portable electronic devices (e.g., Blackberries) are particularly vulnerable to theft or misuse. As noted above, it does not yet appear common for fund complexes to take steps, such as encryption, to protect data in the event that laptops are stolen. However, some fund complexes require the use of authentication devices on

laptop computers and may also seek to limit the storage of non-public information on laptop computers, so as to make it more difficult for a thief to use a stolen laptop to access a computer network or obtain non-public information.

## Data Destruction and Disposal

*What measures are taken by your complex to ensure the proper disposal and destruction of data?*

Proper disposal of data, whether stored electronically or on paper, can assist in safeguarding personal information. With respect to paper files, many fund complexes routinely shred sensitive documents (normally with crosscut shredders) before disposing of them. With respect to files in storage that are scheduled to be discarded, many organizations have contracted with their storage companies on how such files are to be destroyed.[53]

The need for proper disposal is, of course, not limited to paper-based information, and extends to electronic information (such as that contained on hard drives, backup tapes, and other storage media). It is important to recognize that many electronic files that have been "deleted" by a user are in fact recoverable. Some fund complexes have specific policies regarding the disposal of storage media that contain sensitive electronic information. Common means of destroying electronic information include physical destruction of storage media and electronic "shredding," which refers to a process of repeatedly overwriting the data on the storage medium in question with other data (such as strings of ones and zeros).[54]

Fund groups should be aware that various legal requirements might potentially apply to data destruction and disposal.[55] A full discussion of these requirements is beyond the scope of this Study.

## Other Techniques for Protecting Data and Dollars

*What other measures does your complex use to protect information and assets? What steps does your complex take to educate employees, shareholders, and other individuals about identity theft issues? Has your complex evaluated the costs and benefits associated with various types of identity theft insurance for employees or shareholders?*

In addition to authentication and other techniques discussed above, fund complexes have for many years employed a variety of practical measures that are intended to reduce the risk of an identity thief absconding with shareholder assets. Thus, for example, fund complexes have typically required that proceeds of redemptions requested by telephone or on-line be sent only to the shareholder's address of record or to the shareholder's bank account of record. Similarly, fund complexes have typically imposed "hold periods" on shareholders who seek to change their address or bank account of record. Under some circumstances, for large redemptions, fund complexes have required that additional steps be taken to verify the identity of the redeeming shareholder.

Many financial institutions and other organizations have also historically sought to combat identity theft through sharing of information among themselves and with law enforcement agencies.[56] In the fund industry, ICI Mutual has for many years sponsored a fraud prevention program that assists fund groups in identifying and preventing misappropriation of fund assets by identity thieves and other criminals. ICI Mutual's fraud prevention program includes a database of relevant information on all frauds and attempted frauds reported by insureds

to ICI Mutual since 1992. Insureds regularly use this database in seeking to confirm instances of suspected frauds.

Some financial institutions and other organizations have also engaged in outreach efforts to educate customers and employees about the risks of identity theft. As identity theft has been widely publicized, a number of financial institutions, including some fund groups, appear to have stepped up their efforts to reduce identity theft risks through such outreach efforts.[57] With regard to fund shareholders, these efforts may include providing tips for safeguarding personal information,[58] examples of phishing e-mails and websites, warnings about the dangers of spyware, contact information for reporting incidents of identity theft, and links to helpful organizations and websites.[59] With regard to employees, these efforts may include setting forth specific policies and procedures on maintaining information security and confidentiality, and providing periodic bulletins or training to employees about specific "social engineering" strategies by which perpetrators may seek to obtain sensitive information.

Some organizations are reportedly considering the feasibility of seeking to identify, in advance, specific employees who may be most susceptible to social engineering attempts, or who may be tempted to assist in misappropriation of personal information or customer assets. For example, disgruntled or recently terminated employees have been viewed as potential sources of sensitive information (including mission-critical information).[60] Beyond the relatively obvious categories of employees, some experts have proposed that companies should consider compiling psychological profiles of their employees as a means of establishing the likelihood of employee misconduct.[61]

There are also a number of new technologies that may assist organizations in combating identity theft. Certain software products, for example, are designed to assist in identifying fraudulent websites,[62] and other products are designed to assist organizations in assessing whether their legitimate websites are the targets of pharming attacks. So-called geo-location technologies, as another example, are intended to assist in authenticating users by determining the approximate location of a user and hence the likelihood that the user is who he or she claims to be. Many of these technologies remain in various stages of development, and use of these technologies by fund complexes, or even by financial institutions or other organizations, does not yet appear to be common.

Finally, there are new specialty insurance products now available that are designed to mitigate the effects of identity theft on customers and employees. These "identity theft" insurance products are often marketed to institutional buyers, who may purchase master policies on behalf of employees, customers, or clients who may be victimized by identity theft.[63] At this point, the scope of coverage provided is relatively narrow, the limits tend to be low, and it does not appear that a large number of organizations have yet purchased these types of policies.

# Endnotes

[1] "Facts on Identity Theft," http://www.wholesecurity.com/threat/identity_theft.html. Identity theft has also been the most reported complaint received by the Federal Trade Commission in each of the last five years. "FTC Releases Top 10 Consumer Complaint Categories for 2004," Press Release (Feb. 1, 2005), Federal Trade Commission, *available at* http://www.ftc.gov/opa/2005/02/top102005.htm.

[2] "New Identity Theft Survey Reveals Latest Count of Victims, Need for Greater Protection; First Data and Regions Team to Fight Back," Forbes Magazine (May 17, 2005), *available at* http://www.forbes.com/businesswire/feeds/businesswire/2005/05/17/businesswire20050517005673r1.html.

[3] Identity theft is time-consuming and expensive for its victims and for financial institutions. According to one study, each victim of identity theft spends an average of 600 hours trying to repair the damage and the impact of identity theft on a victim may be felt for up to ten years. "Facts & Statistics," Identity Theft Resource Center, *available at* http://www.idtheftcenter.org/facts.shtml.

[4] *Computer Security Lite* was written for senior management and for legal and compliance personnel. The study was designed to facilitate communications with computer security experts, and to assist fund complexes in identifying specific types of computer security risks and in developing and implementing computer security risk management techniques.

[5] An FTC advisory group has identified various categories of personal information, including physical and online contact information, identifying data, financial account information, preference data, photos, and information about the individual's computer system. *See* "Scope and Categories of the Advisory Committee's Work: Recommendations from the Scope Subgroup," Federal Trade Commission, *available at* http://www.ftc.gov/acoas/categories.htm. Many of these categories are largely irrelevant to fund groups, but may provide a framework for considering how to protect different types of information.

[6] By one estimate, financial institutions lost an estimated $4 billion in 2003 as a result of identity theft. *See* "Facts on Identity Theft," Whole Security, *available at* http://www.wholesecurity.com/threat/identity_theft.html.

[7] *See* FDIC, "Putting an End to Account-Hijacking Identity Theft," at 13 (Dec. 14, 2004), *available at* http://www.fdic.gov/consumers/consumer/idtheftstudy/identity_theft.pdf.

[8] *See, e.g.*, Ponemon Institute, "Lost Customer Information: What Does a Data Breach Cost Companies?" (Nov. 2005), *available at* http://www.pgp.com/library/ponemon_report.html.

[9] For example, CardSystems Solutions Inc., a credit card transaction processing service, recently permitted hackers to gain unauthorized access to information about approximately 40 million credit card accounts. Citing inadequate data security standards, American Express and Visa announced that they would cease to use CardSystems' service, and MasterCard reportedly delivered CardSystems an ultimatum requiring it to satisfy heightened security standards within a certain period of time. *See* "Visa, Amex Cut Ties With CardSystems Due to Breach," ComputerWorld (Jul. 25, 2005), *available at* http://www.computerworld.com/printthis/2005/0,4814,103443,00.html.

[10] This change has manifested itself in online shopping patterns, but appears to have extended to other types of financial transactions as well. *See* "'Tis the season for phishing scams: Survey: Scam e-mails might deter online shopping," MSNBC (Nov. 24, 2004), *available at* http://msnbc.msn.com/id/6560652/. Several surveys have found that large percentages of users have modified their online behavior by, for example, not applying for financial products online or by ceasing to use online transaction systems. Forrester Research, Inc., "Phishing Concerns Impact Consumer Online Financial Behavior" (Dec. 2, 2004), *available at* http://www.forrester.com/Research/Document/Excerpt/0,7211,35677,00.html; Forrester Research, Inc., "Internet Viruses Slow Consumers' Online Activity" (Oct. 4, 2004), *available at* http://www.forrester.com/Research/Document/Excerpt/0,7211,34435,00.html; Gartner G2 "Online Transaction Fraud and Prevention Get More Sophisticated" (Jan. 17, 2002), *available at* http://www.gartnerg2.com/research/rpt-0102-0013.asp; Cyber Security Industry Alliance, "National Survey Finds Voters Near Unanimous in Their Concern About Cyber Security and Looking to Congress for Better Protection" (Jun. 15, 2002), *available at* https://www.csialliance.org/news/press/pr_061505.pdf.

[11] For example, the Fair Credit Reporting Act of 1970, as recently amended by the Fair and Accurate Credit Transactions Act of 2004, governs certain types of consumer reports. The Health Insurance Portability and Accountability Act of 1996 provide protection for medical records. In addition, the Gramm-Leach-Bliley Act of 1999 addressed the protection of personal information held by financial institutions. Information security considerations are also implicated by the Public Company Accounting Reform and Investor Protection Act of 2002 (better known as "Sarbanes-Oxley"), which requires information security and other technological issues to be incorporated into the audit process. *See generally* the Federal Trade Commission's overview of a number of federal and state laws relevant to identity theft issues, *available at* http://www.consumer.gov/idtheft/id_laws.htm.

Many states also have laws that are analogous to various of the federal laws briefly described above. California, for example, enacted the Financial Information Privacy Act of 2003, which is analogous to, but generally more stringent than, the federal Gramm-Leach-Bliley Act. Many states have enacted fair credit report laws and laws pertaining to medical records. Most states also have criminal laws regarding privacy and information security. *See* FTC, http://www.consumer.gov/idtheft/id_laws.htm. According to the FTC, Colorado, the District of Columbia, and the U.S. Virgin Islands are alone among U.S. states and territories in not having identity theft laws. *See id.*

These laws tend to provide specific protections to personal information as used by a given industry (e.g., the financial services and heath care sectors), rather than broadly protecting certain types of personal information. "Breach Points Up Flaws in Privacy Laws," New York Times (Feb. 24, 2005), *available at* http://www.nytimes.com/2005/02/24/business/24datas.html?ex=1267333200&en=075426bb36c33ce7&ei=5090&partner=rssuserland.

[12] In December 2004, the SEC adopted two revisions to Regulation S-P, commonly referred to as the "safeguard rule" and the "disposal rule." The "safeguard rule" requires that policies and procedures regarding the protection of consumer records and information be committed to writing. The "disposal rule" requires reasonable measures (such as the burning or shredding of paper documents and erasure or destruction of electronic records) to protect discarded nonpublic personal information about consumers from unauthorized access and use. In general, funds and their advisors, distributors, and transfer agents were required to comply with these rules by July 1, 2005. *Disposal of Consumer Report Information*, Investment Company Act Rel. No. 26685, 69 FR 71322 (Dec. 2, 2004).

At the same time, the FDIC issued a report on "account hijacking," a form of identity theft, based on its study of fraudulent activity perpetrated against bank checking accounts. The FDIC report discusses various methods that financial institutions can employ to protect customer information and prevent, detect, and resolve incidents of account hijacking or other forms of identity theft.

[13] Other countries, such as Japan and certain Western European countries, have enacted consumer information privacy laws, which are often more stringent than analogous U.S. laws. *See*, *e.g.*, "Data Protection: Hot Data," The Economist (Jun. 23, 2005), *available at* http://www.economist.com/displaystory.cfm?story_id=4107024.

[14] The California's Database Security Breach Notification Act of 2003 mandates that, subject to certain exceptions, any business that has suffered, or suspects it has suffered, a computer security breach of unencrypted personal information, must notify all of its California customers of the breach or potential breach. Some privacy experts believe that California's law has influenced similar legislation in many other states. *See* T. Baldas, "Lawyers See Data 'Fear Factor' Rising," The National Law Journal (May 12, 2005), *available at* http://www.law.com/jsp/article.jsp?id=1115802311951. One exception to California's law permits a company that is working with law enforcement on the database breach to refrain from notifying potentially affected individuals of the breach.

[15] Approximately seventeen other states have adopted laws similar to California's. *See*, *e.g.*, "Data Breaches Spur Congressional Action," The Washington Post (July 18, 2005), *available at* http://www.washingtonpost.com/wp-dyn/content/article/2005/07/18/AR2005071800613_pf.html.

[16] *See* T. Baldas, "Lawyers See Data 'Fear Factor' Rising," The National Law Journal (May 12, 2005), *available at* http://www.law.com/jsp/article.jsp?id=1115802311951; T. Zeller, Jr., "Breach Points Up Flaws in Privacy Laws," The New York Times (Feb. 24, 2005), *available at* http://www.nytimes.com/2005/02/24/business/24datas.html?ex=1267333200&en=075426bb36c33ce7&ei=5090&partner=rssuserland (noting that ChoicePoint notified consumers on a nation-wide basis only after it became known that ChoicePoint had informed California residents of a breach).

[17] *See*, *e.g.*, Cyber Security Industry Alliance, "National Survey Finds Voters Near Unanimous in Their Concern About Cyber Security and Looking to Congress for Better Protection" (Jun. 15, 2002), *available at* https://www.csialliance.org/news/press/pr_061505.pdf (reporting that 71% of U.S. voters believe that new Internet consumer privacy laws are needed).

[18] For example, with the Identity Theft Penalty Enhancement Act of 2004, Congress stiffened penalties for perpetrators of identity theft. T. Zeller, Jr., "Personal Data for the Taking," New York Times (May 18, 2005) *available at* http://www.nytimes.com/2005/05/18/technology/18data.html.

In the aftermath of recent data losses, a number of U.S. senators and representatives have introduced data security bills that would, similar to California's law, require disclosure of breaches resulting in the loss of personal information about individuals. *See*, *e.g.*, "Data Breaches Spur Congressional Action," The Washington Post (Jul. 18, 2005), *available at* http://www.washingtonpost.com/wp-dyn/content/article/2005/07/18/AR2005071800613_pf.html. For example, one proposed measure would, if enacted, impose fines of up to $11 million for each undisclosed loss of personal information about 1,000 or more individuals. A recently introduced bill, supported by the ICI, would, if enacted, create uniform national standards governing the protection of sensitive consumer information and the notification required if such information is compromised. *See* Financial Data Protection Act of 2005, H.R. 3997, 109th Cong. (2005).

[19] *See*, *e.g.*, *Harrington v. Choicepoint Inc.*, No. 2:05-cv-01294-MRP-JWJ (C.D. Cal. filed Feb. 22, 2005).

[20] In the past few years, many of the lawsuits on data security issues have been dismissed because plaintiffs have been unable to demonstrate that they suffered actual damages. *See*, *e.g.*, "Class-action TriWest lawsuit dismissed," The Business Journal Phoenix (Oct. 21, 2003), *available at* http://phoenix.bizjournals.com/phoenix/stories/2003/10/20/daily20.html (noting that a class action lawsuit against Tri-West Healthcare Alliance had been dismissed because no actual damages had been demonstrated). Some recently instituted lawsuits may put pressure on the actual damages issue. *Kehoe v. Fidelity Federal Bank & Trust*, D.C. Docket No. 03-80593-CV-DTKH (11th Cir. filed Aug. 26, 2005) (reversing a lower court ruling that the federal Driver's Privacy Protection Act did not require proof of actual damages to recover liquidated damages.). To the extent that the mere release of information is viewed as a harm in and of itself, this issue may undergo some evolution in the coming years.

[21] *See* T. Baldas, "Lawyers See Data 'Fear Factor' Rising," The National Law Journal (May 12, 2005), *available at* http://www.law.com/jsp/article.jsp?id=1115802311951.

[22] In this lawsuit, a company, Ahlo, Inc., is seeking to recover from Bank of America for amounts illicitly wired from Ahlo's Bank of America account. The lawsuit appears to allege that the wire transfer resulted from a "spyware"-type virus that was introduced into Ahlo's computer and that transmitted Ahlo's account number and password for its Bank of America account to an identity thief, who then used this information to effect a wire transfer in Ahlo's name but without Ahlo's knowledge. *Ahlo, Inc. v. Bank of Am. Corp.*, No. 05-2538-CA27 (Fla. Cir. Ct. filed Feb. 3, 2005).

The plaintiff appears to be arguing that Bank of America, having created an online banking system and having allegedly "enticed and induced" Ahlo and other customers to use it, then took on an obligation to safeguard its customers' use of online banking by taking appropriate steps to educate its customers about the risks of online banking and the measures that customers could take to reduce the risks. The plaintiff's arguments even intimate that the bank's obligations extend to taking reasonable steps to secure transactions that customers may effect with the bank (for example, by requiring use of "two-factor" authentication).

[23] Indeed, some experts have expressed concern that a media and public focus on electronic fraud may deflect attention away from the continuing issue of "traditional" fraud. "Online Banking Gets Bad Rap," TechNewsWorld (Mar. 21, 2005), *available at* http://www.technewsworld.com/story/41042.html.

[24] *See*, *e.g.*, "The Weakest Link," PC Magazine (Mar. 16, 2004), *available at* http://www.pcmag.com/article2/0,1759,1537426,00.asp.

[25] *See id.*

[26] *See* "Database Security Best Practices," Security Magazine (Aug. 1, 2005), *available at* http://www.securitymagazine.com/CDA/ArticleInformation/features/BNP__Features__Item/0,5411,157413,00.html (listing recent database breaches). In one case alone – CardSystems – it has been estimated that the security of information about 40 million credit card customers was breached. *See* "Visa, Amex Cut Ties With CardSystems Due to Breach," ComputerWorld (Jul. 25, 2005), *available at* http://www.computerworld.com/databasetopics/data/story/0,10801,103443,00.html.

[27] "Phishing attacks skyrocket in 2004," CNET.com (Dec. 6, 2004), *available at* http://news.com.com/2100-7349_3-5479145.html.

[28] *See* "Phishers Sinking to New Lows: Scammers Now Impersonate Small Financial Institutions," The Washington Post, F05 (Aug. 28, 2005), *available at* http://www.washingtonpost.com/wp-dyn/content/article/2005/08/27/AR2005082700231.html (reporting data from Gartner, Inc. that, from May 2004 to May 2005, 1.98 million Americans lost $2.4 billion to phishing scams).

[29] *See* FDIC, "Putting an End to Account-Hijacking Identity Theft," at 9 (Dec. 14, 2004), *available at* http://www.fdic.gov/consumers/consumer/idtheftstudy/identity_theft.pdf; "MasterCard to take action over phishing attacks," PC Pro (Jun. 23, 2004), *available at* http://www.pcpro.co.uk/news/59509/mastercard-to-take-action-over-phishing-attacks.html.

[30] *See* "Phishers Sinking to New Lows: Scammers Now Impersonate Small Financial Institutions," The Washington Post, F05 (Aug. 28, 2005), *available at* http://www.washingtonpost.com/wp-dyn/content/article/2005/08/27/AR2005082700231.html.

[31] "Phear of Pharming," The Washington Post (Mar. 14, 2005), *available at* http://www.washingtonpost.com/wp-dyn/articles/A33457-2005Mar14.html.

[32] Another means of pharming may occur on an individual user's own computer if a type of spyware is introduced that modifies the "hosts" file (which automatically translates domain name requests into numeric IP addresses). *See, e.g.*, "Beware of ungracious hosts," ZDNet UK (Apr. 11, 2005), *available at* http://reviews.zdnet.co.uk/software/internet/0,39024165,39194577,00.htm.

[33] "DNS 'pharming' attacks target .com domain," ComputerWorld (Apr. 1, 2004), *available at* http://www.computerworld.com/securitytopics/security/hacking/story/0,10801,100813,00.html?source=NLT_SEC&nid=100813.

[34] There is, of course, an overlap between computer security programs (which are broadly concerned with the protection of the electronic hardware and software for information collection, storage, and processing) and data security programs (which are broadly concerned with the protection of information, regardless of whether or not such information is in electronic form).

[35] The most used encryption algorithms, such as AES, Triple DES, and Blowfish, are extremely strong and require an extraordinarily long time to crack using "brute force" methods (*i.e.*, trying every password combination). As a practical matter, these algorithms are all but unbreakable with today's computing power, given a sufficiently strong password. "Advanced Encryption Standard (AES): Questions and Answers," Computer Security Division, Computer Security Resource Center, The National Institute of Standards and Technology, *available at* http://csrc.nist.gov/CryptoToolkit/aes/aesfact.html ("Assuming that one could build a machine that could recover a DES key in a second (i.e., try 255 keys per second), then it would take that machine approximately 149 thousand-billion (149 trillion) years to crack a 128-bit AES key. To put that into perspective, the universe is believed to be less than 20 billion years old.").

[36] *See* 2005 CSI/FBI Computer Crime and Security Survey, at 16, *available at* http://www.gocsi.com/ (noting that 46% of the organizations surveyed encrypted files).

[37] *See id.* (noting that 68% of the organizations surveyed encrypted data in transit).

[38] *See, e.g.*, "Customer Data Lost, Citigroup Unit Says: 3.9 Million Affected As Firms' Security Lapses Add Up," The Washington Post (Jun. 7, 2005), *available at* http://www.washingtonpost.com/wp-dyn/content/article/2005/06/06/AR2005060601682.html; "CitiFinancial Drops Backup Tapes After Data Loss," Enterprise Storage Forum.com (Jun. 6, 2005), *available at* http://www.enterprisestorageforum.com/continuity/news/article.php/3510481 (reporting CitiFinancial's plans to replace backup tapes with electronic transmission of encrypted data).

[39] Under California law, it is unclear what level of encryption strength is required for a company to be able to avail itself of the exclusion. *See* Database Security Breach Notification Act of 2003. Other states may include similar provisions in their analogous laws.

[40] Geotrust (http://www.geotrust.com), for example, relies on this authentication procedure.

[41] Nonetheless, because the services rely on information that is known by the credit reporting agencies and potentially by other third parties as well (such as ChoicePoint), these services do not offer complete security.

[42] Verizon, for example, will not permit a customer to recover a forgotten PIN number over the Internet, but will send a new PIN number to the customer's cell phone.

[43] *See* "Wire Transfer Brouhaha: BofA Suit Sparks Debate In Banking Circles," U.S. Banker (Apr. 2005), *available at* http://www.us-banker.com/article.html?id=20050401W0MNDYJG.

[44] It is unclear how broadly Bank of America intends to offer two-factor authentication (i.e., whether retail customers will be able to use two-factor authentication).

[45] "A New Key to Fighting Identity Theft," The Washington Post (Aug. 28, 2005), *available at* http://www.washingtonpost.com/wp-dyn/content/article/2005/08/27/AR2005082700227.html.

[46] The FDIC notes that, as of December 2004, a number of financial institutions either have begun to use or are using two-factor authentication. *See* FDIC, "Putting an End to Account-Hijacking Identity Theft," at 17-19 (Dec. 14, 2004), *available at* http://www.fdic.gov/consumers/consumer/idtheftstudy/identity_theft.pdf.

[47] *See* "Biometrics: From Reel to Real," PC World (May 18, 2005), *available at* http://www.pcworld.com/resource/printable/article/0,aid,120889,00.asp (noting that even biometric authentication measures may be fooled or defeated); "The Failure of Two-Factor Authentication" (Mar. 12, 2005), *available at* http://www.schneier.com/blog/archives/2005/03/the_failure_of.html.

[48] *See* "Two-Factor Authentication Still Strong," eWeek.com (Apr. 11, 2005), *available at* http://www.eweek.com/article2/0,1759,1782435,00.asp.

[49] *See*, *e.g.*, FDIC, "Putting an End to Account-Hijacking Identity Theft," at 22 (Dec. 14, 2004), *available at* http://www.fdic.gov/consumers/consumer/idtheftstudy/identity_theft.pdf; FDIC, Financial Institution Letters, "Guidance on How Financial Institutions Can Protect Against Pharming Attacks" (Jul. 18, 2005), *available at* http://www.fdic.gov/news/news/financial/2005/fil6405a.html.

[50] *See* "Photos to Fight Phishing?" The Washington Post (May 27, 2005), *available at* http://blogs.washingtonpost.com/securityfix/.

[51] There are a number of different audits – SAS 70, ISO 17799, and CobiT – that organizations may use to assess the data security practices and procedures of various service providers and business partners. *See*, *e.g.*, www.sas70.com/about.htm and linked pages for additional information on SAS 70 audits; Jonathan G. Gossels, *ISO 17799: Pay Attention to This One*, SystemExperts Corporation (2001), *at* http://www.systemexperts.com/tutors/17799.pdf. In addition, some organizations use the Control Objectives for Information and Related Technology ("CobiT"), developed by Information Systems Audit and Control Association ("ISACA"), for their audits.

[52] *See* "Controversial new ID badge: Privacy concerns worry employees," Federal Times.com (Jan. 24, 2005), *available at* http://federaltimes.com/index.php?S=612330 (noting that many federal agencies are adopting the use of RFID cards); "Can't Hide Your Prying Eyes: New technologies can monitor employee whereabouts 24/7, but CIOs must be prepared for the backlash," ComputerWorld (Mar. 1, 2004), *available at* http://www.computerworld.com/securitytopics/security/privacy/story/0,10801,90518,00.html; "Elementary school nixes electronic IDs," CNET.com (Feb. 17, 2005), *available at* http://news.com.com/Elementary+school+nixes+electronic+IDs/2100-1029_3-5581275.html (use of RFID cards in elementary school was dropped after parents protested).

[53] Iron Mountain, for example, offers its customers secure shredding of documents. *See* http://www.ironmountain.com/services/sol3.asp?svc1_content=3&svc2_code=8&sol3_key=6.

[54] Typically, many passes of writing random data are required before the information is deemed to be unrecoverable from the storage medium. Electronic shredding tends to be a slow process, especially if more passes are used. *See* "Answer Line: Wipe Your Drive Clean of All Its Sensitive Data," PC World (Jun. 2003), *available at* http://www.pcworld.com/howto/article/0,aid,110338,00.asp.

[55] For example, in December 2004, the SEC adopted rule amendments under Regulation S-P requiring financial institutions to adopt policies and procedures to safeguard customer information and to properly dispose of consumer report information. *Disposal of Consumer Report Information*, Investment Company Act Rel. No. 26685, 69 FR 71322 (Dec. 2, 2004).

[56] The Financial Services Information Sharing and Analysis Center (http://www.fsisac.com/), InfraGard (http://www.infragard.net/), the Anti-Phishing Working Group (http://www.antiphishing.org/), and the Identity Theft Assistance Corporation (http://www.identitytheftassistance.org/home/index.cfm) are examples of organizations whose members cooperate in order to combat identity theft. Some companies have also sought to combat identity theft by filing lawsuits against phishing operations. *See* "Microsoft Files 117 Phishing Lawsuits: Software giant seeks to find, punish large-scale scam operations," PC World (Mar. 31, 2005), *available at* http://www.pcworld.com/resource/printable/article/0,aid,120258,00.asp; "Microsoft, Amazon file phishing, spamming lawsuits," ComputerWorld (Sep. 28, 2005), *available at* http://www.computerworld.com/printthis/2004/0,4814,96226,00.html.

[57] For example, at least one fund complex has issued a press release warning of the need to protect personal information and suggesting that shareholders teach their children to do so as well. *See* "Identity Theft Bill May Cause Funds Headaches," Ignites (Jul. 11, 2005), *available at* http://www.ignites.com/home/members/print.article.html?id=974226609.

[58] Fidelity Investments, for example, provides information to its customers on maintaining information and computer security (*see* http://personal.fidelity.com/myfidelity/daily/?refhp=pr).

[59] For example, the Identity Theft Resource Center, at http://www.idtheftcenter.org, and the Federal Trade Commission, at http://www.ftc.gov, may be helpful resources to individuals who believe that their personal information has been compromised.

[60] *See, e.g.*, "The Weakest Link," PC Magazine (Mar. 16, 2004), *available at* http://www.pcmag.com/article2/0,1759,1537426,00.asp.

[61] *See, e.g.*, J.T. Turner and M.G. Gelles, THREAT ASSESSMENT: A RISK MANAGEMENT APPROACH, at 132 *et seq.* (2003).

[62] Various types of scanning software, for example, may be used to search the Internet for websites that appear to be those of a legitimate financial institution, but are, in fact, being used in a phishing attack. FDIC, "Putting an End to Account-Hijacking Identity Theft: Study Supplement," at 5 (Jun. 17, 2005), *available at* http://www.fdic.gov/consumers/consumer/idtheftstudysupp/idtheftsupp.pdf. In addition, server log analysis software can be used to detect various types of potentially fraudulent activity and identify accounts that may have been hijacked. *See* FDIC, "Putting an End to Account-Hijacking Identity Theft," at 17-19 (Dec. 14, 2004), *available at* http://www.fdic.gov/consumers/consumer/idtheftstudy/identity_theft.pdf.

[63] The cost of these policies typically depends on the number of employees, customers, or clients covered. Premiums for such policies may be as low as a few dollars per employee per year, and the limits appear to be modest (in the $1,000 to $25,000 range). Moreover, the scope of coverage is relatively narrow, with the policies designed to reimburse identity theft victims primarily for certain types of "nuisance" expenses that they incur in repairing their credit and clearing their names. "Some employers offer ID theft coverage," USA Today (Sep. 11, 2005), *available at* http://www.usatoday.com/money/workplace/2005-09-11-id-theft-benefit_x.htm.

There are also identity theft policies for individuals. For example, many credit card issuers and homeowner insurance policies provide some level of identity theft protection. *See*, *e.g.*, "Providers push insurance covering theft of identity: Skeptics say fears trump facts," Boston.com, *available at* http://www.boston.com/business/articles/2005/02/06/providers_push_insurance_covering_theft_of_identity/ (noting that many companies charge an annual premium of around $25 for $15,000 to $25,000 of coverage, while others include the cost in their standard homeowners policies); "Insurers profit from your identity-theft fears," MSN.com (Jul. 21, 2005), *available at* http://moneycentral.msn.com/content/Banking/FinancialPrivacy/P121558.asp.

## ICI Mutual | *an uncommon value*

**Aligned Interests:**
owned by, governed by and operated for mutual funds and their advisers, directors and officers

**Mutual Fund Knowledge and Expertise:**
tailored, innovative coverage combined with expert claims handling

**Stability and Financial Strength in All Markets:**
consistent coverage and strong capital

ICI Mutual is the predominant provider of D&O/E&O liability insurance and fidelity bonding for the U.S. mutual fund industry. Its insureds represent more than 60% of the industry's managed assets. As the mutual fund industry's captive insurance company, ICI Mutual is owned and operated by and for its insureds. ICI Mutual's services assist insureds to identify and manage risk and defend regulatory enforcement proceedings and civil litigation.

ICI Mutual also serves as a primary source of industry information regarding mutual fund insurance coverage, claims, risk management issues, and litigation developments. Publications include an extensive library of risk management studies addressing such topics as corporate action processing, investment management compliance, computer security, defense cost management, identity theft, and independent direction litigation risk, among others, and the *Investment Management Litigation Notebook*, risk manager alerts, and the annual *Claims Trends* newsletter. Additional services include peer group profiles, coverage analyses, and assistance to insureds and their counsel in litigation defense.

ICIMutual
*A Risk Retention Group*

**ICI Mutual Insurance Company, a Risk Retention Group**
1401 H Street NW, Suite 1000
Washington, DC 20005

800.643.4246
info@icimutual.com