Stop Identity Theft — From the Inside Out

Resource Type: Articles

Topic: Data Privacy, Tech Risk, Cybersecurity, HR Risk and Employment Practices

Masters of disguise are using others' identities to support lavish lifestyles. Using one or two verifiable pieces of data identity, thieves construct a life for themselves and commit someone else's money to supporting it. Armed with name, address, Social Security number, credit cards and PINs (personal identification numbers) stolen from personnel files, office waste baskets and electronic databases, thieves are racking up thousand of dollars against other people's business accounts.

Professional thieves hit hard and fast. Many of them have inside contacts who gather data on current and past employees for a price. These staffers might be someone in senior management, clerks or counselors in the HR department, clerical floats or temporary staff. Motivated by making a quick buck, the thrill of getting away with something, or getting back at someone who's harmed them, they hand over another's identity to criminals. But none of their reasons for engagement protect your nonprofit should the person whose identity was stolen decide to file a suit alleging your nonprofit was negligent in protecting personal privacy. What can serve in your defense are strong internal controls that show you're fulfilling your duty of care in protecting personal information gathered in the course of providing your services.

The first thing to do is make a list of the categories of people whose information you collect:

- paid staff
- volunteer staff, including board members
- service recipients
- donors
- other

Then identify:

- what you collect
- why you collect it
- when you collect it
- where it is stored
- who has access to the information
- how you protect the privacy of the information

Analyze the results to discover where the holes are and plug them. Simply make the identity theft less easy to accomplish, or "harden the target" in today's parlance. Balancing the needs and rights of a nonprofit against its employees and its clients can be tricky. Creating use policies, educating people on their existence and chastising those who break a policy go a long way towards providing necessary protection. And keep in mind that the greatest security risk a nonprofit faces is from disgruntled insiders — not the contract person cleaning the office in the evening or a teenage hacker seeking access to your systems for the thrill factor.

Protect Against the Theft of Personal Information

- Never leave current or former personnel files in an unlocked cabinet or on desktops where they could be perused or stolen. Doing so is likely to be considered negligent if your nonprofit faces a claim of

negligence by a victim of identity theft.

- Carefully guard documents that contain personal data about employees. If these documents aren't to be saved under your document retention policy, they should be destroyed. Never discard these materials intact.
- Review the storage of personal information on your networked computers to make certain that any sensitive files are password protected. Remember that passwords for these documents, as well as other passwords used to restrict access, should be changed at least every six months.
- Discuss information security with all vendors that have access to employee information to make certain that protecting personal information against theft is a top priority of those companies.
- Restrict access to sensitive online and paper files by employees who are about to be terminated.
- Include in your personnel policies a provision indicating that employees are strictly prohibited from attempting to open or access restricted files that contain personal information about other employees or clients unless access to such information is part of an employee's job responsibilities. Employees who violate this rule will be subject to discipline, up to and including termination.
- Develop an information sheet to distribute to employees who believe they are the victim of identity theft. The material should contain the telephone numbers of the fraud departments for the major credit bureaus, and tips for reporting suspected identity theft to the local police, Federal Trade Commission, banks, and credit bureaus. The document should emphasize the importance of prompt action by employees to prevent further theft. Additional resources are available from the FTC at: www.ftc.gov/idtheft.

Risk Management Strategies to Protect Client Privacy

- Articulate your nonprofit's policy concerning client privacy and instruct all staff on the policy.
- Provide periodic updates to paid and volunteer staff in order to keep all personnel abreast of changes in record keeping and documents destruction policies.
- Promptly investigate any allegations that client privacy has been compromised, and document these investigations.
- Contact your nonprofit's legal counsel if you believe privacy has been compromised and seek independent advice in conducting an investigation.
- Discipline any staff member, including volunteers, who have violated the nonprofit's privacy policy.
- Examine policy violations carefully to determine whether the nonprofit can take any steps to prevent future violations.
- Obtain permission before using photographs or other information about clients for public relations or marketing purposes. Always obtain a signed photo release form before including photos of your clients in an annual report or on your Web site. Exercise extreme caution when using photos of children for any purpose. Don't provide any information that could help identify the child.
- If your nonprofit maintains detailed files that contain highly personal information about your clients, restrict access to these files to those individuals whose job requires them to use the files. In some organizations highly personal information should be kept separate from information that several persons in the nonprofit may need to view from time to time. For example, monthly progress reports concerning a mentor-mentee relationship may be accessible by several departments within the organization, while the results of the initial intake process, including answers to highly personal interview questions, may not.
- Keep your systems secure, and let employees know that the need to maintain client privacy is the job of everyone. Change system passwords on a regular basis (every 60 to 90 days), and keep regular audit trails of information accessed on your database. When telecommuting employees leave the organization, change the access phone numbers into your system to prevent unauthorized entry.
- Remember to consider your website as you identify steps your nonprofit can take to protect client privacy. Some nonprofits interact with clients via their websites, while others have customers or clients where the only interaction with the client is through the website. If you collect personal client information through your website, develop a statement that addresses how you protect the security and confidentiality of this information.