



# ID-ology: A Planner's Guide to Identity Theft

by Jo Day and Kevin Day

**W**e recently received an e-mail from our Internet provider containing information on how to prevent identity theft. This got us thinking: How many financial advisors have broached this topic with their clients? When a client's identity is stolen, their financial advisor should be one of the first calls they make. And rightly so—you should be someone they both notify and turn to for help.

Identity theft occurs when someone uses your personal information, without your knowledge, to commit fraud or a crime. Not only can identify theft harm your clients' financial situation, but other aspects of their life as well.

According to 2003 statistics from the Federal Trade Commission, depending on the type of fraud committed, it took an average of 30–60 hours of a victim's time and \$500–\$1,200 out-of-pocket cost to recover from identify theft. And that's not to say the individual's identity or credit rating is restored to the same good standing they had before the theft occurred. Many people don't have the patience, resources, or time it takes to restore their good financial name. Considering your advisory role, this is a scenario in which your client service skills should shine.

So, what's a financial advisor to do? What will you do when you receive a call from a panicked client who thinks their financial identity may be compromised?

## Face Facts

First, recognize that, at some point, one of your clients will become an identity theft

“First, recognize that, at some point, one of your clients will become an identity theft victim.”

victim. Last year, the FTC reported nearly ten million people had their identities compromised, and as you'll read below, criminals are becoming increasingly creative and organized. Just consider how many sources store your personal information—from gym memberships to shopping reward cards. While the feeling that “it won't happen to me” may be your initial reaction or that of your clients, “there is no business model to prevent identity theft,” according to Bob Hartle, identity theft victim turned victims' rights advocate. It is truly a matter of when your number comes up.

Just ask Gary Gardner, owner of Legacy Wealth Advisors in Walnut Creek, California, who's had three family members hit by identity theft within a six-month period. First, his father-in-law's ATM pin number was intercepted before it arrived in the mail, resulting in maximum daily withdrawals from his bank account for several days before the problem was identified. Another thief attempted to purchase a car using his son's credit. By the time the fraud was detected, the thief had written over \$30,000 in bad checks by setting up a fraudulent checking account, and the thief successfully filed and received a tax refund in the son's name. Finally, Gardner's daughter's paycheck became much slimmer when a man fraudulently filed a spousal support claim, resulting in

withholding of a portion of her wages by both the state and the county.

Beyond doing the basics with which everyone is familiar (for example, shredding financial information with a cross-cut shredder, not carrying your Social Security number in your wallet), there are ways advisors and advisory firms can help manage identity theft.

## Raise Client Awareness

Ten years ago, Gardner discovered that one of his physician clients was a victim of identity theft when comparing the client's Social Security wage statement with his tax return. Says Gardner, “the client made \$250,000 and the Social Security statement said \$25,000.” Originally thinking it was an error, they discovered after further investigation, that an employee within the medical group's third-party billing service was selling Social Security numbers.

Based on his personal experiences, Gardner developed an Identity Theft module to deliver to each of his clients. The module includes an action item checklist (posted, along with other resource information, at [www.trumpetinc.com/idtheft.jsp](http://www.trumpetinc.com/idtheft.jsp)) for clients to use to protect their identities. Other good suggestions to review with clients are available at [www.fightidentitytheft.com](http://www.fightidentitytheft.com). Accord-

ing to Gardner, the key to getting his clients to implement the suggestions has been his following up to ensure each item on the checklist has been accomplished.

While consumers may begin to request free annual credit reports later this year (the southwest region of the country is first to be eligible in December 2004),<sup>1</sup> many sources suggest that checking your credit once a year is not good enough. Some advisors encourage their clients to sign up for a credit monitoring service to receive weekly e-mail alerts when there have been inquiries in or changes to their credit (for example, a new line of credit has been opened, or a record of late payment). Each of the three main credit bureaus (Transunion, Equifax, or Experian) offers their own monitoring service, which only reports activity from their respective

bureau. Cost ranges from \$80 to \$120 a year and includes different features. TrueCredit offers a one-time single report from all three credit bureaus for \$35.00 at [www.truecredit.com](http://www.truecredit.com).

Hartle also recommends that clients check their children's credit and Social Security wage statement each year from the day they are first issued a Social Security number. Without these checks, criminals can lucratively use minors' Social Security numbers for years to commit fraud before your child ever applies for credit.

### What to Do When It Happens

Bob Hartle turned his ordeal with identity theft into a personal crusade. In addition to

providing educational speaking, his non-profit educational organization helps victims of identity theft for free and has a resource guide available at [www.idfraud.org](http://www.idfraud.org).

Should identity theft happen to a client, Hartle recommends the following immediate actions:

1. Obtain a police report specific to identity theft. Hartle explains that a report simply for theft or fraud is not good enough. Should the local police department not understand the difference, Hartle's guide spells it out.
2. Notify one of the three major credit bureaus of fraudulent activity. By law, when one bureau is notified, it must notify the other two.
3. Check with the state's department of

*"Sure, I know I should have professional liability coverage for the risks I face everyday. But as a small business owner, I also need to be able to afford it."*



**EZ Insurance Solutions®**

Protecting Financial Services Professionals

Provided by the industry leaders in financial services professional liability:

**AON CNA**

### The affordable solution for Tax & Financial Services Professionals:

**EZ Insurance Solutions® Professional Liability Insurance** is specifically designed for your **small business needs**, and the increased liability risks of your profession.

Surprisingly affordable rates are tailored to the services your business provides.

\* For qualified products only.

- Flexible annual coverage limits from \$100,000/\$250,000 up to \$1 million/\$2 million to pay for legal defense and settlement.
- Cost is based on the size of your firm as well as services provided. **Great for sole practitioners, small firms or part timers.**
- Coverage can be adjusted by endorsement for financial planning services you may provide.
- Premium credits start after just a year.

Get a **FREE**, no-obligation rate quote by applying online at [www.ezinssolutions.com](http://www.ezinssolutions.com) or call toll-free: **1-866-225-8464**

EZ Insurance Solutions is a service mark of Affinity Insurance Services, Inc. In CA, MN, and OK, AIS Affinity Insurance Agency, Inc. (CA License #0795465) and in NY and NH, AIS Affinity Insurance Agency. CNA is a service mark and trade name registered with the US Patent and Trademark Office. The program referenced in this ad is underwritten by Continental Casualty Company, one of the CNA companies. This information is for illustrative purposes only and is not a contract. It is intended to provide a general overview of the products and services offered. Only the policy can provide the actual terms, coverages, amounts, conditions and exclusions. All coverages not available in all states. A specimen policy is available upon request.

©2004 All right reserved.

NA-504hJFP

motor vehicles to see if any fraudulent IDs or driver's licenses have been issued in your name. If so, request that a fraud alert be placed on the national computer, which will help get the criminal arrested.

4. Obtain a copy of your work history from the Social Security Administration and notify them if there are any errors.

### Doing Your Part to Protect

While businesses agree that identity theft is a problem, states Hartle, most of them are not doing much, if anything, to help prevent the problem. All of the following are good policies and procedures for your firm to put in place to prevent your firm from becoming a source for identity theft.

**Screen out potential problems.** Because many employees are frequently friends or relatives of existing employees, many firms still do not perform criminal or credit background checks on employees. For minimal cost and time (check out the service offered at [www.personnelprofiles.com](http://www.personnelprofiles.com)), you can be satisfied that a potential employee does not have an issue that could cause problems down the road.

Just because you hire an employee via a temporary agency, don't assume the agency does adequate due diligence. Hartle indicates that criminals increasingly seek employment at health-care, billing, and financial firms where they can access personal information. A temp agency that does not properly screen provides a nice loophole for them. When hiring temporary employees or key vendors who will have access to your clients' information, ask for evidence that the firm performs background checks on their hires.

When outsourcing services such as transcription, be sure to refer to the client by using a client code rather than using their name.

When an employee leaves the firm,

make it part of your exit checklist to change passwords. When new employees join the firm, ensure they sign a privacy policy statement and provide confidentiality training, discussed below.

### Protecting Data

**Confidentiality training.** Develop a training session to bring employees up to speed on disclosing personal information; otherwise, they could unwittingly hand out information while thinking they are servicing the client. For example, if an unfamiliar person (such as "assistant to the client's accountant") calls to confirm information, the employee should take down the request, get a call-back phone number, and check with the client before supplying any personal information to an outside party.

**Encrypt confidential information sent via e-mail.** Since e-mail is such a convenient means of sending documents, ensure that your staff knows how to generate password-protected PDFs of files containing confidential information they send via the Internet. Software such as Attach Plus ([www.attachplus.com](http://www.attachplus.com))<sup>2</sup> or the full version of Adobe Acrobat ([www.adobe.com](http://www.adobe.com)) has this functionality.

California state law SB 168 (currently in effect) makes it illegal for businesses to transmit a Social Security number over the Internet unless the connection is secure or the Social Security number is encrypted. Because California is often the model for other states' legislative efforts, keep this in mind when e-mailing tax returns or account forms as attachments.

#### Keeping information out of view.

Ensure that your server's backup media is password protected and that employees log out of their computers each evening. Train employees to lock up any client work in progress from view of a cleaning service. Use encryption software to store your passwords instead of writing them on sticky notes on your computer. There are many

inexpensive options to choose from at [www.spychecker.com/software/pass.html](http://www.spychecker.com/software/pass.html).

Trust is arguably your most important asset as a financial advisor. Helping your clients protect their personal information deserves serious focus in your service model. Make sure that your clients know the steps you are taking to protect their information and that you can help them if they do become a victim of identity theft.



### Endnotes

1. Consumers may request free credit reports annually beginning December 1, 2004, in western states; March 1, 2005, in midwestern states; June 1, 2005, in southern states; and September 1, 2005, in eastern states. Currently, residents of Colorado, Maryland, Massachusetts, New Jersey, and Vermont are entitled by state law to one free report from a credit reporting agency per year. Residents of Georgia are entitled to two. Other circumstances also entitle consumers to a free credit report (for example, if they are denied credit based on information in their credit report or if they are a fraud victim).
2. Attach Plus was developed by Kevin in response to feedback we received from financial planners in our consulting business.

---

*Jo Day and Kevin Day are principals of Trumpet Inc. in Phoenix, Arizona. They provide technology consulting and services to financial planning firms via the Internet. They can be contacted at [info@trumpetinc.com](mailto:info@trumpetinc.com) or <http://www.trumpetinc.com>.*