As a trusted financial planner, part of your role is to protect client assets and safeguard their privacy. This is an opportunity for you to advise clients on protecting their personal privacy, preventing identity theft, and suggesting proven strategies to greatly reduce their risks.

A recent survey by Privacy Concierge LLC indicated nearly 65 percent of respondents earning more than $175,000 annually felt personal privacy risk and identity theft were very serious concerns.

Javelin Strategy & Research reports that an American becomes a victim of identity theft every two seconds. According to Creditsesame.com, losses from identity (ID) theft totaled $24.7 billion in 2012. The Bureau of Justice Statistics claims ID theft caused $1,769 of direct and indirect losses per person.

ID theft and personal privacy are intertwined but distinct. Personal privacy extends to clients not wanting entities or people to have access to personal data, whereas ID theft prevention relies on restricting access to personal data that can be used to impersonate or steal financial or health care resources.

Hundreds of databases used by financial institutions, lawyers, private investigators, collection agencies, employers, business competitors, and the general public provide various types of personal information and detailed reports for purchase. Some of this personal information can be used for identity theft and some can be used to locate assets for investigations and lawsuits. This information can easily be purchased by anybody and potentially be used to locate people, their families, or to impersonate someone.

**Types of ID Theft**

Identity theft goes beyond stealing a credit card to fraudulently make charges. These are the primary types of identity theft:

**Financial identity theft.** This is when the victim’s bank accounts and credit cards are accessed and used illegally. A thief can withdraw money or max out credit cards. The victim’s identity may be used to originate loans, get new credit cards, and open new accounts. This affects a client’s credit report, which can be devastating and difficult to remedy.

**Driver’s license identity theft.** Criminals find ways to use a stolen driver’s license, including selling it to someone who looks passably similar to the real ID owner. If somebody is caught for a traffic violation—drunk driving or another drug-related charge—using a stolen driver’s license, they don’t have to show up in court and now the police are looking for the person whose ID was stolen. Now the victim’s driving record has these offenses, which may lead to having a revoked or suspended driver’s license, an outstanding warrant for arrest, or an increase in car insurance rates.

**Social Security and IRS identity theft.** Thieves use victims’ Social Security numbers for both financial and non-financial theft and impersonations. Tax refund fraud is the fast-growing tax crime and the IRS is struggling to control its growth. This involves using a Social Security number and other personal identifying information, including past addresses, to claim a tax refund on behalf of the victim. In a 2012 Department of Treasury Inspector General report, the IRS is predicting to lose $21 billion from tax refund fraud alone. If you’re an ID theft victim, or think you may have had personal identifiable information stolen, you may file an Identity Theft Affidavit form 14039 with the IRS to offer further protection. The IRS allows for a 6-digit Identity Protection Personal Identification Number to be assigned to prevent tax refund fraud (see www.irs.gov/Individuals/Get-An-Identity-Protection-PIN).

**Medical identity theft.** Thieves use the victim’s identity to make false health insurance claims. The danger of medical identity theft, as the World Health Organization (WHO) points out, is that this could lead to incorrect entries in the victim’s medical history. Erroneous entries could lead to incorrect diagnosis and other complications as well as unpaid deductibles and co-pays.

**Child identity theft.** A common assumption is that a minor’s identity would be of little value. Actually, it is the opposite. A child’s information and Social Security number may be used to defraud the government, create documents, commit crimes, and apply for loans.

**Synthetic identity theft.** This type of identity theft uses several victims’ personal identifying information to...
create a new identity. This can be used for opening loans, lines of credit, and various types of new accounts.

**The Security Freeze**

The greatest tool in preventing information from being stolen and used illegally is the security freeze. Under federal law, a security freeze requires a credit reporting agency to lock down the credit file and it can only be opened with specific permission and PIN code assigned to the client. This can generally be done for little or no cost for victims of identity theft.

There are three well-known credit bureaus: Experian, Equifax, and Transunion. However, there are over a dozen additional "specialty" bureaus, which include non-financial and financial firms. These companies use personally identifiable information to track, monitor, and report on individuals. It’s recommended to place a freeze on those as well. Some of these other bureaus are used for banking, insurance, specialized lending, utilities and renting property. Information in the reports may include:

- Public records of criminal or civil cases
- Credit history
- Bankruptcy filings
- Companies with which you have an existing or prior business relationship (insurance companies or banks)
- Medical information
- Driving records and vehicle ownership information
- Employment history with current and past payroll details
- Marriage and divorce details

Placing a security freeze on the more than 16 credit and information bureaus stops most ID theft in its tracks and makes it nearly impossible to open many types of credit, banking, and/or insurance accounts without the potential victim giving specialized access or using their PIN code to unlock the specific bureau.

Your client can request fraud alerts on their credit bureaus, but these typically need to be renewed every 90 days, are not a long-term solution, and are not as effective as a security freeze. In some cases, victims of identity theft may have an extended fraud alert placed for seven years, but a security freeze is more effective and secure.

Consumer reporting agencies, which are not credit reporting agencies, do not provide security freezes. They may, however, allow a short statement to be placed on the file—which can be used as an extra layer of security—that can be customized. For example, your clients could have a statement placed on a Medical Information Bureau (MIB) file warning of potential fraud and to verify two forms of photo ID and call specific phone numbers to verify identity. This would help prevent an ID thief opening medical insurance in the victim’s name and using it or selling it for use by someone else. The MIB has more than 400 insurance companies reporting medical information for insurance purposes.

**Use a Private Mailbox**

Your clients should never use their home address because that information is sold to marketing lists and becomes public information. Having your home address on your car registration opens you up to being robbed by the crafty valet who can clone your garage door opener or the thief who stole your purse with your home information on all your documents.

Better options include opening a postal box (not a P.O. box) that can accept mail or packages and provide a street address with suite; a private mailbox (PMB) which can be a UPS Store or similar service; or virtual mailboxes like Earth Class Mail (earthclassmail.com) that provide remote mail services to review, remotely open, and scan mail through email. The PMB should be used on everything personal from driver’s licenses, auto registration, utilities, credit card statements, and anything shipped.

Multiple ID theft protection firms provide credit monitoring services—including reviewing various databases for use of credit, banking, and personal identifying information—that will notify the potential victim and assist in fixing the damage from the thieves. Firms include LifeLock, Identity Guard, IdentityForce, and TrustedID. Many similar services range from $100 to $300 annually that provide various levels of notification when a potential victim’s information is being used or sold.

**Protect Against Hackers**

Another concern is hackers accessing bank, credit card, and email accounts via usernames and passcode data by individual or hacker websites.

Avoid being hacked by using a two-factor authentication, which involves using a username and password plus a secondary level of security, such as security codes sent via text. Find out if the websites you sign into most use two-factor authentication at this website: twofactorauth.org.

Also, always use a Virtual Private Network (VPN) service when using public WiFi. And be cautious. Simple security breaches occur due to carelessness such as checking email at a hotel business center or airline club lounge computer and not closing out the email session.

Information security and privacy is predicated on a foundation of basic steps to reduce access to information. Find additional information regarding ID theft prevention at Privacy Rights Clearinghouse (www.privacyrights.org), and Electronic Frontier Foundation (www.eff.org).

Geoffrey VanderPal, DBA, CFP®, has been active in the financial advising industry since 1992 and owns a privacy consulting firm, Privacy Concierge LLC. Contact him at gvanderpal@theprivacyconcierge.com.