

Identity Crisis

>> Your data—and your clients' data—are at risk

By Chuck Green

Ann Bracci figures she dodged a bullet. When someone helped themselves to her laptop that she briefly left in the outer area of an office, Bracci knew it could be in the hands of someone intent on pilfering precious nuggets of her client's personal information—as well as hers. Fortunately, she stored no confidential data on the computer, but the potential ramifications made Bracci shudder.

A REALTOR® with Gallagher & Lindsey, Inc.® REALTORS, Alameda, Bracci takes no chances with her new machine. "I always carry it on my shoulder. Now my husband and colleagues think I'm too cautious," she chuckles.

No way, notes Regina P. Brown, a REALTOR® with R.P. Brown Real Estate, San Luis Obispo. "[Identity theft] is an out of control problem. Thieves are one step ahead of the law."

How Big Is the Risk?

Last November, the Federal Trade Commission released a survey showing that 8.3 million American adults, or 3.7 percent of all American adults, were victims of identity theft in 2005. Of those, 3.2 million experienced misuse of their existing credit card accounts; 3.3 million experienced misuse of non-credit card accounts; and 1.8 million found that new accounts were opened or other frauds were committed using their personal identifying information.

The Privacy Rights Clearinghouse (www.privacyrights.org/identity.htm) has documented that more than 165 million records from various entities have been compromised since January 2005. In 2006, identity fraud accounted for more than \$55 billion in

losses, according to a Javelin Strategy & Research (www.javelinstrategy.com) Survey in February 2007.

Identity theft prevention is difficult, says Steve Orduño, a Certified Identity Theft Risk Management Specialist, Paso Robles. "There are always going to be individuals who will take advantage of people's good nature and lax attitude."

Those characteristics are perfect fodder for identity theft rings that Brown says are operated by international crime rings; many of them are headquartered overseas, making them virtually untouchable by U.S. law enforcement agencies. Brown, who also is a Certified Identity Theft Risk Management Specialist and teaches a DRE-approved course called "Identity Theft: Protect Yourself, Your Clients, Your Business," explains that most thefts are committed by those hacking into laptops and procuring information in bulk,

Continued on page 29



CLASSIFIEDS

SOFTWARE

Agent Business Builder™ Classified Simplified Pro™

real estate software



1-800-581-1943

www.powermatecorp.com

See You In Court!

Continued from page 20

Plaintiffs' Lawyers. While many licensees do act as professionals, there are still scores of agents that are undereducated, or putting the deal before their client. Take real estate courses and read and understand the forms you're using. Review preliminary title reports carefully and as soon as possible. While you may not fully understand the information, tell your client to have it checked out with the title company if there is a question. Avoid situations that could lead to two contracts. Exercise the utmost care with multiple offers, backup offers, and contingencies.

The agent is under a duty to use reasonable care and skill in his work and to follow the instructions of his client. A court described the dilemma facing those who work for commissions and are fiduciaries as follows: "Under this compensation system few brokers are immune to the temptation to consider their financial interests from time to time while they are advising clients. Being at once a salesman and counselor is too much of a burden for most mortals." ♦

Fredric W. Trester is a C.A.R. Strategic Defense Panel Attorney and a partner with Manning & Marder, Kass, Ellrod, Ramirez.

**Provided by the Strategic Defense Program at C.A.R. The program is committed to providing timely and important information to help REALTORS® with risk management and avoid litigation. To further protect yourself, consider the C.A.R.-endorsed E&O insurance provided by AIG. For more information, call (213) 739-8379.

Identity Crisis

Continued from page 25

including social security numbers, job information, and birth dates, which they sell online. She adds that clients who become victims of identity theft due to a real estate agent's "negligence" can sue the agent, the broker, and the office.

Agents must take it upon themselves to bone up on tactics used by identity thieves and make "good faith efforts" to thwart them, adds Orduño. One way is to minimize transport of customer data. "How many agents go home with piles of folders in their back seat or trunk of their car to work on them over the weekend?"

At the same time, to help shield themselves against possible reverberations of identity theft, real estate offices should establish written policies and ensure their agents are familiar with them, he says. Consequently, should information be lost, an office can provide documentation that its agents have been briefed on proper procedures.

Some tactics used by identity thieves that REALTORS® and their offices can be vulnerable to:

>>Shoulder surfing, i.e., peering over someone's shoulder, which Orduño calls a "low-tech way to steal high-tech information."

>>Dumpster diving: "I spoke to a person who had recently been released from incarceration for ID theft using this tactic," notes Orduño. The victim? A county sheriff's department.

>>Phishing, i.e., where consumers are duped into entering personal information via a bogus e-mail or Web site.

>>Skimming, i.e., a method by which thieves quickly and temporarily steal a credit card and run it through a skimmer, a device that reads credit card information.

Preventive Steps

Real estate offices should provide their agents access to attorneys who specialize

in real estate law in order to address their inquiries regarding identity theft, states Brown. She notes that doing so is a component of offering a legal membership plan so agents don't have to pay every time they need to ask a question.

>>Initiate a clean desk policy: "When you go to lunch, remove items from your desk and place them under lock and key." Orduño also recommends shutting down your computer.

>>Cross-cut all mail and other documents to be disposed of, in both your office and home office.

>>Protect your home office: Designate a room in your house exclusively for office use and keep the door locked when away, says Brown. "Your children might have friends over, and someone might go into your office and use your computer." That raises the potential for the theft of private client and personal information.

>>Convert paper files into an electronic file, such as a CD, and place it in a safety deposit box.

>>Store all client documents, including loan applications, bank letters, copies of checks, credit reports, and escrow information, in a locked file cabinet.

>>Beware of discarded copiers and fax machines: "People don't think about it when they copy materials on a copy or fax machine, but most of them have built-in scanners, which scan the information to a computer disk." That can be particularly dicey when an office disposes of a machine, adds Brown, who notes when you donate computers, information can be extracted off the hard drive. ♦

Chuck Green is a freelance real estate writer.

HELPFUL SITES

- www.ftc.gov/bcp/edu/microsites/idtheft/
- www.ftc.gov/os/2007/09/P075418idtheft.pdf
- www.ssa.gov/pubs/idtheft.htm