



October 2006

Legal Update

A WRA Publication Exclusively for the Designated REALTOR®

Please Route to:

Inside This Issue

2

How ID Thieves Obtain Personal Information

3

How ID Thieves Use Personal Information

4

Use of Personal Information in RE Transactions

6

What You Can Do to Help Prevent ID Theft

8

Assisting Identity Theft Victims

10

ID Theft Prevention

13

Hotline Questions

14

ID Theft Resources



WISCONSIN REALTORS® ASSOCIATION

© 2006

Protecting Against Identity Theft

Buying or renting a home or apartment invariably involves sharing a certain amount of personal information with third parties, leaving consumers at risk. Both purchasers and renters need to be cautious. When buyers provide personal information online to a network of mortgage lenders or other real estate professionals, they may be authorizing the owners of the site to share or sell that information to third parties.

Tenant applicants are also asked for a great deal of private information, which landlords use for screening prospective tenants. REALTORS® should urge their clients and customers to be careful and not indiscriminately share personal information online, over the phone or in person.

The home buying or renting process can become a nightmare for consumers who discover they have a credit report that is tainted through identity theft (ID theft) or fraud. People whose identities have been stolen can spend anywhere from months to years – and thousands of dollars – cleaning up the mess the thieves have made of a good name and credit record. In the meantime, victims of ID theft may lose job opportunities, be refused loans for education, housing, or cars, and even get arrested for crimes they didn't commit. Victims of ID theft experience humiliation, anger, and frustration as they tackle the process of rescuing and restoring their identity.

ID theft is a traumatic experience that often endangers a consumer's ability to purchase a property. REALTORS® are in an excellent position to pro-

vide additional value to their clients and customers by helping them prevent ID theft and by having resources available to help people deal with ID theft should it occur. REALTORS®, including landlords with rental properties, may also reevaluate the information that they ask of consumers, eliminating unnecessary information and carefully safeguarding and disposing of personal identification information in their files and records.

This *Legal Update* overviews the incidence of ID theft in Wisconsin and nationally, the techniques most commonly used to take private identifying information, and the personal devastation often resulting from this crime. A discussion of what REALTORS® and others can do to prevent ID theft tracks the steps for securing personal identifying information when a business keeps such data in its records, how to properly dispose of this information and the procedures that must be followed if there is a security breach and personal identifying information is comprised. Ways to assist ID theft victims are also discussed and tips for preventing ID theft are reviewed. The *Update* concludes with a list of Hotline questions and answers pertaining to ID theft issues.

Incidence of Identity Theft National Statistics for 2005

The Federal Trade Commission (FTC) received over 685,000 consumer complaints during calendar year 2005 concerning the Internet, distance selling and related violations – 63 percent represented fraud and 37 percent

Contacts

EDITORIAL STAFF

Author

Debbi Conrad

Production

Terry O'Connor

ASSOCIATION MANAGEMENT

Chairman

Jeff Kitchen, CRS, GRI

President

William E. Malkasian, CAE

ADDRESS/PHONE

The Wisconsin
REALTORS® Association,
4801 Forest Run Road,
Suite 201
Madison, WI 53704-7337
(608) 241-2047
(800) 279-1972

LEGAL HOTLINE:

Ph (608) 242-2296
Fax (608) 242-2279
Web: www.wra.org

The information contained herein is believed accurate as of 9/22/2006. The information is of a general nature and should not be considered by any member or subscriber as advice on a particular fact situation. Members should contact the WRA Legal Hotline with specific questions or for current developments.

Reproduction of this material may be done without further permission if it is reproduced in its entirety. Partial reproduction may be done with written permission of the Wisconsin REALTORS® Association Legal Department.



**WISCONSIN
REALTORS®
ASSOCIATION**

© 2006

were ID theft complaints. ID theft occurs when someone appropriates an individual's personal identification information, such as a Social Security number (SSN) or credit card account number, to commit fraud or theft. Credit card fraud (26%) was the most common form of reported ID theft followed by phone or utilities fraud (18%), bank fraud (17%), and employment fraud (12%). Other significant categories of ID theft reported by victims were government documents/benefits fraud (9%) and loan fraud (5%). "Electronic Fund Transfer" related ID theft was the most frequently reported type of ID theft bank fraud during calendar year 2005.

The FTC believes that ID theft is grossly under reported and estimates that 10 million Americans are the victims of ID theft each year. Approximately 100,000 cases of ID theft are believed to go unreported each year in Wisconsin. The FTC estimates that Americans lost \$5.5 billion dollars in 2005 as the result of ID theft, with the losses to Wisconsin consumers believed to be around \$50 million each year.

2005 Wisconsin Data

In Wisconsin there were 7,215 fraud complaints and 2,782 ID theft complaints filed with the FTC in 2005. Credit card theft accounted for 26 percent of the complaints, followed by phone or utilities fraud (20%), bank fraud (18%), employment-related fraud (10%), government documents/benefits fraud (6%) and loan fraud (5%). Approximately 18 percent of these victims experienced more than one type of ID theft.

When broken down by age, the 18- to 29-year-old range was hit the hardest, with 29 percent of the complaints, followed by the 30- to 39-year-olds with 24 percent, the 40- to 49-year old group with 20 percent, the 50- to 59-year-old group with

13 percent and the 60 and over group with 9 percent. Five percent of the ID theft complaints were made by people under 18 years of age.

Of the major metropolitan areas nationwide, the Chicago-Naperville-Joliet area ranked 19th with 9,534 ID theft-related complaints (102.1 complaints per 100,000 population) while the Milwaukee-Waukesha-West Allis area ranked 35th with 1,141 complaints (75.3 per 100,000 population) and the Minneapolis-St. Paul-Bloomington area ranked 36th with 2,307 complaints (74.8 complaints per 100,000 population).

On a state-by-state basis, Wisconsin ranks 39th for ID theft, measured by the 2,782 ID theft complaints (50.3 per 100,000 population) filed in 2005. Within Wisconsin, Milwaukee generated the most ID theft complaints in 2005 with 629 complaints, followed by Madison (152), Racine (99), Kenosha (70) and Green Bay (67).

How Identity Thieves Obtain Personal Information

Personal information is generally defined – with respect to ID theft and privacy issues – as a person's last name and first name or first initial in combination with his or her SSN; driver's license number or state identification number; credit, debit or other financial account number; security code, access code or password; DNA profile; or fingerprint, voiceprint or retina or iris image. Other identifying information, which in combination with other personal data may be enough for an identity thief, includes a person's mother's maiden name, ATM pin number or birth date.

Despite one's best efforts to manage the flow of personal identifying information and strictly limit access, skilled identity thieves may use a variety of techniques to access personal data.

- Information from businesses or other institutions is obtained by:
 - Stealing records or information while on the job
 - Bribing an employee with access to these records
 - Hacking these records
 - Conning information out of employees
- They may steal mail, including bank and credit card statements, credit card offers, new checks and tax information.
- They may rummage through trash cans on residential streets, the trash of businesses or public trash dumps – in other words, “dumpster diving.”
- They may get credit reports by abusing their employer’s authorized access to them, or by posing as a landlord, employer, or someone else with a legal right to access credit reports.
- They may steal credit or debit card numbers by capturing the information in a data storage device in a practice known as “skimming.” They may swipe a credit card during an actual purchase, or attach the device to an ATM machine where people enter or swipe their cards.
- They may steal a wallet or purse.
- They may complete a change of address form to divert a person’s mail to another location.
- They may steal personal information found in a home.
- They may steal personal information through e-mail or by telephone, posing as legitimate companies and claiming there is a problem with an account. This practice is known as “phishing” when it happens online, and “pretexting” when it occurs over the phone.

Phishing

Phishing is a high-tech scam that uses spam or Internet pop-up messages to deceive consumers into disclosing their credit card numbers, bank account information, SSNs, passwords, and other sensitive personal information. These Internet identity thieves may claim to be from a business or organization that the consumer regularly deals with, such as a bank, Internet service provider (ISP), online payment service or even a government agency, and send e-mail that warns,

“We suspect an unauthorized transaction on your account. To ensure that your account is not compromised, please click the link below and confirm your identity.”

-- or --

“During our regular verification of accounts, we couldn’t verify your information. Please click here to update and verify your information.”

Some phishing e-mails threaten a dire consequence if the consumer doesn’t respond. The messages direct the consumer to a Web site that looks just like a legitimate organization’s site. It turns out to be a bogus site created to trick consumers into divulging personal information so the identity thieves can steal consumers’ identities and run up bills or commit crimes in the consumers’ names.

Pretexting

Pretexting is the practice of obtaining personal identifying information under false pretenses. Pretexters often sell this personal information to people who may use it to obtain credit, steal assets or even initiate bogus investigations or file merit less lawsuits against an individual.

Pretexters use a variety of tactics to obtain personal information. For example, a pretexter may call, claim he’s from a survey firm, and ask a consumer a few questions. When

the pretexter has the information he wants, he may use it to call an individual’s financial institution, pretending to be that person or someone with authorized access to the account. He might claim that he’s forgotten his checkbook and needs information about his account. In this way, the pretexter may be able to obtain personal information such as a SSN, bank and credit card account numbers, information in a credit report, and the existence and size of the person’s savings and investment portfolios.

Some information, however, may be a matter of public record, such as whether a person owns a home, pays his or her real estate taxes, or has ever filed for bankruptcy. It is not pretexting to collect this kind of information.

By law, it’s illegal for anyone to:

- Use false, fictitious or fraudulent statements or documents to get customer information from a financial institution or directly from a customer of a financial institution.
- Use forged, counterfeit, lost, or stolen documents to get customer information from a financial institution or directly from a customer of a financial institution.
- Ask another person to obtain someone else’s customer information using false, fictitious or fraudulent statements or using false, fictitious or fraudulent documents or forged, counterfeit, lost, or stolen documents.

How Identity Thieves Use Personal Information

“I first was notified that someone had used my SSN for their taxes in February 2004. I also found out that this person opened a checking account, cable and utility accounts, and a cell phone account in my name. I’m still trying to clear up everything and just received my income tax refund after waiting four to five

months. Trying to work and get all this cleared up is very stressful.”

– *From a consumer’s complaint to the FTC, July 9, 2004.*

Once identity thieves have an individual’s personal information, they use it in a variety of ways.

- They may call the individual’s credit card company to change the billing address on the account. The imposter then takes over the account and runs up credit card charges. Because the individual’s credit card bills are being sent to a different address, it may be some time before the individual realizes there is a problem.
- They may open new credit card accounts in the individual’s name. This is true name fraud. When they use the credit cards and don’t pay the bills, the delinquent accounts are reported on the individual’s credit report.
- They may establish phone or wireless service in the individual’s name.
- They may open a bank account in the individual’s name and write bad checks on that account.
- They may counterfeit checks or credit or debit cards, or authorize electronic transfers in the individual’s name, and drain the individual’s bank account.
- They may file for bankruptcy under the individual’s name to avoid paying debts they’ve incurred under the individual’s name or to avoid eviction.
- They may buy a car by taking out an auto loan in the individual’s name.
- They may get identification such as a driver’s license issued with their picture, in the individual’s name.
- They may get a job or file fraudulent tax returns in the individual’s name.
- They may give the individual’s name to the police during an arrest. If they don’t show up for their court date,

a warrant for arrest is issued in the individual’s name.

Many of the activities may continue for many months before the victim begins to discover what has happened. Telltale signs that a person’s identification information may have been misappropriated include:

- Failing to receive bills or other mail. A missing bill could mean an identity thief has taken over the account and changed the person’s billing address to cover his tracks.
- Receiving credit cards that weren’t applied for.
- Being denied credit, or being offered less favorable credit terms, like a high interest rate, for no apparent reason.
- Getting calls or letters from debt collectors or businesses about merchandise or services the person didn’t purchase.

Use of Personal Information in Real Estate Transactions

Real estate brokers and agents, property managers and landlords may often come into possession of consumers’ personal identification information such as their SSNs. In addition, REALTORS[®], landlords and property managers will typically use some consumer report information in their daily practice. For brokers, an buyer’s credit report and a seller’s Comprehensive Loss Underwriting Exchange (CLUE) Report are examples of consumer information reports that may be used in transactions. Landlords and property managers will also likely use credit reports and other reports indicating tenant histories when screening tenants for rental properties. A “consumer report” is generally any report on a consumer’s credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living pre-

pared by or obtained from an agency that collects such information.

Social Security Numbers

The SSN was originally devised to keep an accurate record of each individual’s earnings, and to subsequently monitor the benefits paid under the Social Security program. However, use of the SSN as a general identifier has grown to the point where it is the most commonly used and convenient identifier for all types of record-keeping systems in the United States.

If a person’s SSN falls into the wrong hands, the person may be in for a great deal of hardship and problems if someone else illegally assumes the person’s identity. When a dishonest person has someone else’s SSN, the thief can use it to get other personal information and apply for credit in the person’s name. Thus, consumers can be protected against ID theft if SSNs are only used when absolutely necessary.

Specific laws require a person to provide his or her SSN for certain purposes. A SSN is required or appropriately requested by:

- The Internal Revenue Service (IRS) for tax returns and federal loans
- Employers for wage and tax reporting purposes
- States for the school lunch program
- Banks for monetary transactions
- The Veterans Administration as a hospital admission number
- The Department of Labor for workers’ compensation
- The Department of Education for student loans
- States to administer any tax, general public assistance, motor vehicle or driver’s license law within its jurisdiction
- States for child support enforcement

- States for commercial driver's licenses
- States for the Food Stamps Program
- States for Medicaid
- States for the Unemployment Compensation Program
- States for Temporary Assistance to Needy Families
- The U.S. Treasury for U.S. Savings Bonds

Federal privacy law regulates the use of SSNs by government agencies. When a federal, state or local government agency asks an individual to disclose his or her SSN, the federal Privacy Act requires the agency to inform the person of the statutory or other authority for requesting the information, whether disclosure is mandatory or voluntary, what uses will be made of the information, and the consequences, if any, of a failure to provide the information.

In general, any other request for a person's SSN is not necessary and the individual has the right to refuse. However, that may mean that the person does not receive the item or service for which the number was requested. For example, utility companies and other services ask for a SSN, but they do not need it — they can do a credit check or identify the person in their records by alternative means.

Credit Reports

Landlords and property managers may often use credit reports and other consumer reports to evaluate rental applications. This practice is subject to the Fair Credit Reporting Act (FCRA). The FCRA requires landlords who deny a lease based on information in the applicant's consumer report to provide the applicant with an "adverse action notice."

A consumer report contains information about a person's credit characteristics, character, general reputation, and lifestyle. A report also may

include information about someone's rental history, such as information from previous landlords or from court or eviction files. The FCRA applies to all reports prepared by a consumer reporting agency (CRA) — a business such as a credit bureau, that assembles such reports for other businesses.

The consumer reports used by landlords and property managers may include credit reports from credit bureaus such as Trans Union, Experian, and Equifax or an affiliate company; reports from tenant-screening services that may be based on reports from previous landlords, court records or a credit report the service got from a credit bureau; reports from reference-checking services that contact previous landlords or other parties listed on the rental application; and reports from agencies that verify personal, employment and previous landlord references on behalf of the rental property owner.

An adverse action is any action unfavorable to the rental applicant, such as denying the application, requiring a co-signer, requiring an extra or larger deposit, or charging higher rent. When an adverse action is taken based solely or partly on information in a consumer report, the FCRA requires the landlord or property manager to provide notice of the adverse action to the applicant. The adverse action notice is required whenever the information in the consumer report played any role in the adverse action, no matter how minor — the consumer report need not be the main reason for the decision and may be one of several factors. The notice must include:

- The name, address and telephone number of the CRA that supplied the consumer report (including a toll-free telephone number for CRAs that maintain files nationwide);
- A statement that the CRA that supplied the report did not make the adverse action decision and thus cannot give reasons for it; and,

- A notice of the applicant's right to dispute the accuracy or completeness of any information furnished by the CRA, and to receive a free report from the CRA upon request within 60 days.

If credit reports are obtained about some tenant applicants, they should be obtained for all. In Wisconsin, Wis. Admin. Code § ATCP 134.05(4) permits a landlord to charge an applicant up to \$20 to cover the landlord's actual cost of obtaining a credit report if the information is coming from an accredited national credit-reporting agency. The landlord must provide the applicant with a copy of the report and may not charge an applicant who provides the landlord with a credit report that is less than 30 days old. Note, however, that local ordinances in the cities of Madison and Fitchburg prohibit charging the tenant for any credit report.

CLUE Reports

A CLUE report is another type of consumer report used in real estate purchase transactions to learn about past damages to the property being purchased. CLUE is a loss history information database developed by and used by insurance companies that contains a record of the calls made to insurance companies related to damage to that property, including any flood or hailstorm damage, and any other claims made within the last five years. CLUE Home Seller's Disclosure Reports can be ordered only by home sellers, and do not display personal information that a home seller may wish to keep private, such as name, SSN and date of birth. Sellers may order CLUE reports online from www.choicetrust.com.

For more information about CLUE reports, see the "Wisconsin Homeowner's Insurance" Resource Page" online at www.wra.org/insurance.

What Real Estate Brokers, Landlords and Property Managers Can Do to Help Prevent ID Theft

Real estate professionals can help reduce the risk of ID theft for the consumers they work with by safeguarding all personal information in their files, by properly disposing of consumer report information records, and by minimizing the personal information collected in the first place.

Data Protection

With ID theft and mortgage fraud on the rise, the security and privacy of consumer data in real estate transactions is a concern. Companies would be well served by implementing computer data security policies to induce consumer trust and protect themselves from lawsuits. Nobody wants to be the real estate broker who has to face a group of homeowners or the property manager facing a group of tenants to let them know that a laptop computer or office files were stolen containing their homes' listing information or tenant screening data, along with other personal information.

Computer and Internet Policies

Since so much information is stored on computers, basic computer safety policies can help protect any personal data within the system from being pirated by identity thieves.

1. Virus Protection. Virus protection software must be installed on all computers and updated regularly to protect against intrusions and infections that can lead to the compromise of computer files or passwords. Ideally, virus protection software should be set to automatically search for and install updates each day or at least each week. The software should also be set to scan the system for viruses each week, if not more frequently.

2. Don't Open Unknown Attachments or Click on Unfamiliar Links. No one

should open files sent by strangers, or click on hyperlinks or download programs from people they don't know. Everyone should be careful about file-sharing programs because this is one way to expose a computer system to a computer virus or "spyware," which can capture passwords or any other information typed on a keyboard. Computer users should never download Web programs from untrustworthy sources, open e-mail from unknown people, or bring in software that someone gave them. These are dangerous practices that can lead to spyware intrusions and phishing attacks, which use bogus e-mail messages to trick people into giving up bank account or other personal information.

3. Anti-Spyware Program. Spyware can change the appearance of Web sites, alter settings, cause poor system performance and collect information from a computer. Certain spyware can actually capture bank account numbers, SSNs and other information and send them back to the spyware originator. An anti-spyware program is a necessity.

4. Firewall. A firewall program is also an important security measure, especially if a high-speed Internet connection like cable or DSL leaves the computer connected to the Internet 24 hours a day. The firewall program will stop uninvited access. When there is no firewall, hackers can take over a computer, access personal information or use the computer to commit other crimes.

5. Data Encryption. Use a secure browser that encrypts or scrambles information you send over the Internet and be sure the browser has the most up-to-date encryption capabilities. Brokers and others should encrypt files on their computer's hard drive – especially with laptop computers – so that if the computer itself is stolen, the files won't be as accessible. The encryption tool

enables users to set up and encrypt certain folders so that only specified persons can view them, or encrypt certain pieces of communication to hide more sensitive information, such as when homeowners are away from their houses for showing times.

6. Put Passwords on Laptops. Try not to store financial information on laptops. If it is absolutely necessary, use a strong password with a combination of letters (upper and lower case), numbers and symbols. Don't use an automatic log-in feature that saves your user name and password, and always log off when you're finished. That way, if a laptop is stolen, it's harder for a thief to access personal information.

7. Computer Disposal. Before disposing of a computer, delete all the personal information it stored. Deleting files using the keyboard or mouse commands or reformatting your hard drive may not be enough because the files may stay on the computer's hard drive, where they may be retrieved easily. Use a "wipe" program to overwrite the entire hard drive.

8. Back Up Data. Computer data should be backed up on a weekly basis, at the least. Individual agents can back up data on CDs, while those who have multiple computer users should consider backing up data on a separate hard drive.

9. Keep Files and Laptops Physically Secure. Ensure the physical security of files, laptops and PDAs – lock them up. Stolen laptops are a huge risk because they are so easily taken and may contain a wealth of personal information which is very attractive to an ID thief. Do not leave laptops in the office on weekends or in hotel rooms when traveling. Lock them in a secure place or at least hide them out of site.

10. Screen and Train Employees. Run background checks on employees who have access to personal information. Make sure all staff mem-

bers follow all office policies protecting consumer privacy, which should include such rules as not asking for personal data in front of others, computer security and shredding old files.

Disposing of Consumer Report Information

Most consumers consider the information about them contained in a credit report, CLUE Report or tenant rental application private and confidential, and the FTC agrees with them. In an effort to maintain consumer privacy, protect against unauthorized access and protect against ID theft, the Fair and Accurate Credit Transactions Act of 2003 (FACT Act) regulates the use of consumer report information. The FTC's Disposal Rule regulates how individuals and businesses dispose of sensitive consumer information when it is no longer needed.

The FTC Disposal Rule protects consumer report information, that is, consumer reports and the information derived from them. This includes credit reports, credit scores and CLUE Reports as well as the reports that businesses or individuals receive with information relating to a person's employment background, check writing history, tenant history or medical history.

The FTC Disposal Rule applies to all individuals and entities that use consumer report information. Real estate brokers, lenders, insurers, credit bureaus, employers, landlords, property managers, government agencies, collection agencies, mortgage brokers, attorneys and private investigators, for example, all must comply.

The Disposal Rule allows organizations and individuals to determine what measures are reasonable based on the sensitivity of the information, the costs and benefits of different disposal methods, and changes in technology. Although the Disposal Rule applies only to consumer report information, the FTC encourages those who dispose


of any records containing any personal or financial consumer information to take similar protective measures.

Reasonable measures for disposing of consumer report information include:

- Burning or shredding papers so that the information cannot be read or reconstructed;
- Destroying or erasing electronic files or media so that the information cannot be read or reconstructed;
- Hiring a document destruction contractor to dispose of consumer report information material after conducting a due diligence review of the contractor's qualifications, reputation and integrity.

Consumer Information Disposal for REALTORS®

To comply with the FTC rule you must establish policies and procedures for the proper disposal of consumer information that protect against unauthorized access. While burning or pulverizing information may sound like more fun, most REALTORS® will shred consumer report information. Crosscut shredders are the best choice because standard shredders are not as effective in blocking reconstruction of the consumer information. Electronic media – such as computer hard drives and floppy disks – should be destroyed or completely erased. Throwing a computer into the trash is not acceptable unless the hard drive is destroyed. Using a document destruction contractor is obviously an effective way to handle the situation.

 **REALTOR® Practice Tips:** The best practice is to apply the new federal rules to all records kept in the office (and at home if ID theft is a concern). After seven years have passed, most attorneys are comfortable recommending that old files be destroyed.

For more information about the FACT Act and the FTC Disposal Rule, visit the FTC Web site

at www.ftc.gov/bcp/conline/pubs/alerts/disposalalrt.htm.

Wis. Stat. § 895.505, Wisconsin's "dumpster diving" law, similarly provides guidelines for the disposal of records containing personal information. It applies, however, only to medical businesses, tax preparation businesses and financial institutions.

Don't Collect Unneeded Personal Information

One of the best ways to protect a business' most valuable assets – its clients and customers – is to not collect personal identifying information that is not really needed. Brokers and landlords may be well served to evaluate whether all of the information that they collect is really necessary. Limit contact information collected to what is needed to efficiently conduct business and avoid asking for other personal or financial information unless there is a specific purpose. Collection of financial information in a real estate transaction, for instance, may be left to lenders and financial institutions.

SSNs are considered confidential and are required to be given only for specific government uses such as income and tax reporting. More and more consumers are reluctant to give their SSNs and may question why this information is needed.

Real estate brokers, for instance, do not need the SSNs of their customers and clients in their records. SSNs come into play at closing when the parties may simply write their SSNs directly onto the Wisconsin Real Estate Transfer Tax Return.

Sellers may also provide their SSNs directly to the closing agent who will need the SSNs for filing Form 1099-S with the IRS. The closing agent may ask for the seller's SSN before or at closing and the seller is legally required to give his or her SSN or other tax identification number and certify that it is correct. The closing agent

may use the IRS form W-9, Request for Taxpayer Identification Number and Certification, for this purpose.

Property managers and landlords may also wish to evaluate their rental application forms and determine whether they absolutely need to have all of the personal information that is presently requested. They may wish to discuss with their CRAs what identifying information is needed to effectively obtain consumer reports and in particular assess whether SSNs and birth dates must be requested. Property managers and landlords must balance the need to properly screen tenants — for financial and safety reasons — with the tenants' need to not indiscriminately give out personal identification data.

Assisting Identity Theft Victims

ID theft is an insidious crime. ID theft victims may not discover that their personal information has been compromised until several months have passed. One way an individual often discovers he or she is a victim of ID theft is by discovering new credit accounts opened by the identity thief in the individual's name. This is often detected in the individual's credit report or when the person starts receiving bills or notices for unauthorized purchases or loans made by the ID thief.

The harm to a consumer's credit and daily life can be devastating. Victims of ID theft often have trouble getting new credit cards or loans because of the damage to their credit ratings. They often also need to get new driver's licenses, SSNs and bank accounts, all of which can be daunting and overwhelming to the elderly and other vulnerable consumers. As if clearing one's financial standing were not enough, some victims of ID theft must also clear their personal reputations because the ID thief has committed crimes in

the victim's name. Recovery from the ID theft may take many years.

Wisconsin's Data Breach Notification Law

If a Wisconsin business experiences a data breach and consumers' personal identifying information is stolen or falls into the hands of potential thieves, it is important for the company to act quickly to investigate the situation and notify those consumers who may be at risk. Wis. Stat. § 895.507 requires most government agencies and businesses operating in Wisconsin that maintain personal information about individuals who reside in Wisconsin, to notify those individuals if an unauthorized person has acquired their personal information.

The law defines personal information as an individual's last name and first name or first initial, in combination with the SSN; driver's license or state identification number; financial, credit or debit account number, security or access code or password; DNA profile; or a fingerprint, voiceprint, retina or iris image.

Businesses that conduct business in the state and maintain personal information in the ordinary course of business are among those who are required to give notice whenever an unauthorized person acquires personal information held by the business. This includes Wisconsin brokers and landlords. However, no notice is required if the unauthorized acquisition does not create a material risk of ID theft or fraud, or if the information was acquired in good faith by an employee or agent and is used for a lawful purpose.

Notice must be given to the ID theft victims no later than 45 days after the business learns of the unauthorized acquisition of personal information. The notice must be given by mail or by a method that the entity has previously used to communicate with the victim (for example,

e-mail). In cases where the personal information of more than 1,000 individuals was acquired, the business from which the information was taken must also notify all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, for example, the three major credit reporting agencies.

A law enforcement agency may request that the business delay providing notice in order to protect an investigation or homeland security. For additional information, visit the Wisconsin Office of Privacy Protection Web site at privacy.wi.gov.

For FTC information and policies regarding an information compromise, visit www.ftc.gov/bcp/edu/pubs/business/idtheft/bus59.htm.

What to Tell Victims of ID Theft

If any client or customer believes that his or her personal identifying information has been stolen and put to unauthorized use, REALTORS® can provide guidance and point the consumer to those agencies and resources established to provide assistance to victims of ID theft.

The following are the basic steps for the victim to take when ID theft has occurred:

1. Credit Card Companies and Financial Institutions. If the stolen information impacts financial accounts, close compromised credit card accounts immediately. Consult with your financial institution about whether to close bank or brokerage accounts immediately or first change your passwords and have the institution monitor for possible fraud. Place passwords on any new accounts. Avoid using your mother's maiden name, your birth date, the last four digits of your SSN, your phone number, or a series of consecutive numbers.

The ID Theft Affidavit makes it easier for consumers to dispute debts resulting from ID theft. The ID Theft Affidavit is a model form that can be used to report information concerning the ID theft, simplifying the process of alerting companies where a new account was opened in the victim's name. Developed by the FTC in conjunction with banks, credit grantors and consumer advocates, the ID Theft Affidavit is accepted by participating credit issuers, retailers, banks, and other financial institutions. Log on to www.ftc.gov/bcp/conline/pubs/credit/affidavit.pdf or call 1-877-ID-THEFT for a copy of the ID Theft Affidavit.

2. National Credit Bureaus. Contact the fraud departments of each of the three nationwide consumer reporting companies and place an initial fraud alert on your credit reports. This alert can help stop someone from opening new credit accounts in your name.

- Equifax: 1-800-525-6285; www.equifax.com; P.O. Box 740241, Atlanta, GA 30374-0241
- Experian: 1-888-EXPERIAN (397-3742); www.experian.com; P.O. Box 2002, Allen, TX 75013
- TransUnion: 1-800-680-7289; www.transunion.com; Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790

An initial fraud alert stays on the credit report for 90 days. Once fraud alerts have been placed, the ID theft victim is entitled to order free copies of his or her credit reports, and, upon request, only the last four digits of the SSN will appear on the credit reports. It's prudent to wait about a month before ordering the reports because suspicious activity may not show up right away. The reports should be closely reviewed for suspicious activity, like inquiries from companies you didn't contact, accounts you didn't open, and debts on your accounts that you can't explain. Verify that personal informa-

tion such as the SSN, address, name or initials, and employers is correct.

3. Government Identification Documents. If the stolen information includes a SSN, driver's license or other government-issued identification, contact the agencies that issued the documents and follow their procedures to cancel and get a replacement. Ask the agency to flag the file to keep anyone else from getting a license or another identification document in your name.

4. Police Report. File a report with local police or the police where the ID theft took place. Get the report number or a copy of the report in case the bank, credit card company or others need proof of the crime later.

5. Identity Theft Data Clearinghouse. Call the FTC's Identity Theft Data Clearinghouse toll-free at 1-877-ID-THEFT (1-877-438-4338) to report the theft. Complaints received from victims of ID theft via the hotline or the online complaint form ([rn.ftc.gov/pls/dod/wsolcq\\$.startup?Z_ORG_CODE=PU01](http://rn.ftc.gov/pls/dod/wsolcq$.startup?Z_ORG_CODE=PU01)) are entered into the Data Clearinghouse. Counselors will take the complaint and give advice on how to deal with the credit-related problems that could result from ID theft. The Identity Theft Hotline and the Identity Theft Web site (www.consumer.gov/idtheft) give consumers a central place to report the theft to the federal government and receive helpful information.

The Identity Theft Data Clearinghouse is the federal government's database for tracking ID theft complaints. It offers law enforcement officers access to the nation's only central database of ID theft complaints; information on trends in ID theft; and an opportunity to work with other law enforcement agencies and appropriate private organizations. The Identity Theft Data Clearinghouse is part of Consumer Sentinel (www.consumer.gov/sentinel), an online

cyber tool and fraud complaint database used by hundreds of civil and criminal law enforcement agencies in the United States and abroad.

Businesses Must Provide Victims and Law Enforcement with Records Relating to ID Theft

FCRA spells out rights for victims of ID theft, as well as responsibilities for businesses. ID theft victims are entitled to ask businesses for a copy of transaction records — such as applications for credit — relating to the theft of their identity. Victims can authorize law enforcement officers to get the records or ask that the business send a copy of the records directly to a law enforcement officer. The businesses covered by the law must provide copies of these records, free of charge, within 30 days of receiving the request in writing. This means that the law enforcement officials who ask for these records in writing may get them from your business without a subpoena, as long as they have the victim's authorization.

The law applies to a business that has provided credit, goods, or services to, accepted payment from, or otherwise entered into a transaction with someone who is believed to have fraudulently used another person's identification. For example, if a business opened a cell phone account in the victim's name or extended credit to someone misusing the victim's identity, the business may be required to provide the records relating to the transaction to the ID theft victim or the law enforcement officer acting on that victim's behalf.

Businesses may select a specific address to which requests from victims must be mailed. If the business does not have a high degree of confidence that it knows the victim, before providing the records, the business may ask victims for:

1. Proof of identity, which may be a government-issued ID card, the same type of information the identity thief used to open or access the account, or the type of information the business is currently requesting from applicants or customers; and,

2. A police report and a completed affidavit, which may be either the FTC Identity Theft Affidavit (www.ftc.gov/bcp/conline/pubs/credit/affidavit.pdf) or the business' own affidavit.

Credit Report Repair

Once an ID theft victim has received his or her credit reports, they should be carefully reviewed. If fraudulent or inaccurate information is found, it should be removed or corrected.

Correcting Fraudulent Information in Credit Reports

The FCRA establishes procedures for correcting fraudulent information on credit reports and requires that the report be made available only for certain legitimate business needs.

Under the FCRA, both the consumer reporting company (credit bureau) and the information provider (the business that sent the information to the consumer reporting company), such as a bank or credit card company, are responsible for correcting fraudulent information in a credit report. The victim should contact both the consumer reporting company and the information provider to protect his or her rights under the law.

Consumer Reporting Company Obligations

Consumer reporting companies (credit bureaus) will block fraudulent information from appearing on a credit report if the ID theft victim sends them a copy of an ID theft report (www.ftc.gov/bcp/conline/pubs/credit/affidavit.pdf) and a letter (www.ftc.gov/bcp/conline/pubs/credit/BlockingLetter) telling them what information is fraudu-

lent. The letter also should state that the information does not relate to any transaction that the victim made or authorized. In addition, proof of the victim's identity, such as the victim's SSN, name, address, and other personal information requested by the consumer reporting company, must be furnished.

The consumer reporting company has four business days to block the fraudulent information after accepting the ID theft report. It also must tell the information provider that it has blocked the information.

Information Provider Obligations

Information providers must stop reporting fraudulent information to the consumer reporting companies once an ID theft victim sends them an ID theft report and a letter explaining that the information they're reporting resulted from ID theft. The information provider also may not hire someone to collect the debt that relates to the fraudulent account, or sell that debt to anyone else who would try to collect it.

Victim Resources

For additional ID theft victim information, www.consumer.gov/idtheft. The FTC also has comprehensive guidelines for ID theft victims in its "What to Do if Your Identity is Stolen" publication, available online at www.ftc.gov/bcp/conline/pubs/credit/idcrisis.pdf.

ID Theft Prevention

REALTORS® and their clients and customers should stay alert for signs of ID theft and take steps to prevent this crime.

Do not give out your SSN to people or companies that you do not know. Give your SSN only when absolutely necessary, and ask to use other types of identifiers. If your health insurance company uses your SSN as

your policy number, ask to substitute another number.

Before disclosing any personal information, make sure you know why it is required and how it will be used. Don't give out personal information on the phone, through the mail, or on the Internet unless you've initiated the contact or are sure you know whom you're dealing with. Identity thieves are clever, and have posed as representatives of banks, Internet service providers (ISPs) and even government agencies to get people to reveal their SSN, mother's maiden name, account numbers, and other identifying information.

Treat your trash carefully. Shred information you no longer need that contains personally identifiable information and account numbers. To thwart an identity thief who may pick through your trash or recycling bins to capture your personal information, tear or shred your charge receipts, copies of credit applications, insurance forms, physician statements, checks and bank statements, expired charge cards that you're discarding and credit offers you get in the mail.

Guard your mail from theft. Promptly remove your incoming mail from your mailbox. Install a locking mailbox if mail theft is a problem in your neighborhood. Deposit your outgoing mail in post office collection boxes or at your local post office, rather than in an unsecured mailbox. If you're planning to be away from home and can't pick up your mail, have a friend or neighbor pick it up each day or contact the U.S. Postal Service to request a vacation hold. They will hold your mail at your local post office until you can pick it up or are home to receive it. When ordering new checks, pick them up from the bank instead of having them mailed to your home mailbox.

Keep the personal information you have at home and at work in a safe place. Secure personal information in

your home, especially if you have roommates, employ outside help, or are having work done in your home. Keep your purse or wallet in a safe place at work; do the same with copies of administrative forms that have your sensitive personal information.

- ➔ Don't carry your SSN card; leave it in a secure place. Carry only the identification information and the credit and debit cards that you'll actually need when you go out. Do not carry extra credit cards, your birth certificate or passport, or other cards that display your SSN.
- ➔ Place passwords on your credit card, bank, brokerage and phone accounts. Create unique passwords and personal identification numbers (PINs) and avoid using easily available information such as mother's maiden name, date of birth, last four digits of your SSN, phone number or a series of consecutive numbers. When opening new accounts, you may find that many businesses still have a line on their applications for your mother's maiden name. Ask if you can use a password instead.
- ➔ Ask about information security procedures in your workplace or at businesses, doctor's offices or other institutions that collect your personally identifying information. Find out who has access to your personal information and verify that it is handled securely. Ask about the disposal procedures for those records as well. Find out if your information will be shared with anyone else. If so, ask how your information can be kept confidential.
- ➔ You can have your name removed from credit bureau marketing lists and opt out of receiving offers of credit in the mail by calling toll-free to 888-5OPTOUT (888-567-8688) or visiting the Opt Out Web site at www.optoutprescreen.com. The three nationwide consumer reporting companies use the same toll-free number for this function. You will be asked to provide your SSN, which the consumer reporting companies need to match you with your file.
- ➔ Be cautious when responding to promotions. Identity thieves may create phony

promotional offers to get you to give them your personal information. Before you share any personal information, confirm that you are dealing with a legitimate organization. Check an organization's Web site by typing its URL in the address line, rather than cutting and pasting it. Many companies post scam alerts when their name is used improperly. Or call customer service using the number listed on your account statement or in the telephone book. For more information, see the FTC publication, "How Not to get Hooked by a 'Phishing' Scam," online at www.ftc.gov/bcp/conline/pubs/alerts/phishingalrt.pdf.

- ➔ If an identity thief strikes, you might first notice it on your bank or credit card statements. Even if you don't balance your checkbook or pay your credit card bill right away, look at the statement as soon as you get it to see if there are any unauthorized charges or withdrawals. If there are, report them right away. If your bill or statement doesn't come at the normal time, call and ask about it since late arrival could be another indication of ID theft.
- ➔ If you like to surf the Web or purchase items on line, make certain you have adequate security on your computer. Don't click on pop-up ads or open e-mails and attachments from persons you don't know and trust. Install a firewall and virus and spyware protection. Check your browser security settings. Also check the security of the Web site. Generally, "https" and/or a small padlock in the bottom right corner means that the site is secure.
- ➔ In this information age, there is a large market for personal information and some of the companies with which we do business share or even sell our personal information to others. Before purchasing online, check the privacy policy of the business. Also, read the privacy statement that your credit card company sends you. In certain cases, you might be able to opt out of that company sharing all or a part of your information by contacting the company.

Subscribe

This *Legal Update* and other Updates beginning with 92.01 can be found in the members-only legal section of the WRA Web site at: www.wra.org.

A subscription to the *Legal Update* is included in all association Designated REALTOR® dues. Designated REALTORS® receive a monthly publication package including the *Legal Update*, and other industry-related materials.

REALTORS® and Affiliate members may subscribe to the Designated REALTOR® publication package for \$30 annually. Non-member subscription rate for the package is \$130 annually. Member subscription price for the *Legal Update* is \$25, non-member price is \$75. Each subscription includes 12 monthly issues.

Contact the Wisconsin REALTORS® Association to subscribe:

4801 Forest Run Road,
Suite 201
Madison, WI, 53704-7337

(608) 241-2047
(800) 279-1972

www.wra.org



**WISCONSIN
REALTORS®
ASSOCIATION**

© 2006

➔ Get a copy of your credit report from each of the three major credit reporting agencies at least once a year. Review the reports to be sure no one else is using your identity to open new accounts or to use your existing accounts.

Free Annual Credit Report

The FCRA requires each of the nationwide consumer reporting companies – Equifax, Experian, and TransUnion – to provide consumers with a free copy of their credit report, upon request, once every 12 months. The three companies have one central Web site, toll-free telephone number, and mailing address where the free credit report may be ordered. The only authorized Web site is annualcreditreport.com.

Many other Web sites claim to offer free credit reports, scores, or monitoring, but they are not part of the official annual free credit report program. Some of these “imposter” sites come with strings attached or direct consumers to other sites that try to sell something or collect personal information.

To order a free report at annualcreditreport.com, a consumer must provide his or her name, address, SSN and date of birth. If he or she has moved in the last two years, the previous address may also be required. To maintain the security of these files, each nationwide consumer reporting company also may ask for information that only the consumer would know, like the amount of the monthly mortgage payment. Each company may ask for different information. That’s because the information each company has in its file may come from different sources.

Ordering a Free Annual Credit Report

- Online, visit annualcreditreport.com.
- Call toll-free 1-877-322-8228.

- By mail, complete the Annual Credit Report Request Form (www.ftc.gov/bcp/online/include/request-formfinal.pdf) and send it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For more information about free credit reports, go to the FTC information brochure online at www.ftc.gov/bcp/online/pubs/credit/freereports.pdf.

Active Duty Alert Helps Protect Military Personnel from ID Theft

Members of the military away from their usual duty station may place an “active duty alert” on their credit reports to help minimize the risk of ID theft while they are deployed. When a business sees the alert on the credit report, it must verify the person’s identity before issuing any credit. The business may try to contact the person directly, which may be impossible if the person is deployed. Consequently, the law allows the use of a personal representative to place or remove an alert. Active duty alerts are effective for one year, unless

the person requests that the alert be removed sooner. If the deployment lasts longer than one year, a second alert may be placed on the report.

To place an active duty alert on a person’s credit reports, or to have it removed, call the toll-free fraud number of one of the three nationwide consumer reporting companies. The company will require the person to provide appropriate proof of identity, which may include the SSN, name, address, and other personal information.

- Equifax: 1-800-525-6285; <http://www.equifax.com/>.
- Experian: 1-888-EXPERIAN (397-3742); <http://www.experian.com/>.
- TransUnion: 1-800-680-7289; <http://www.transunion.com/>.

Only one of the three companies need be contacted to place an alert — the called company will contact the other two, which will place an alert on their versions of your report as well.

**I am dedicated.
I am experienced.
I am more productive.**

The CRS Designation is the symbol of professionalism and experience in residential real estate. More than 37,000 professionals across the country have the education and transaction requirements needed to be called a CRS. They earn an average of \$160,500 each year, nearly three times more than the \$59,300 earned by the average REALTOR® who sells residential real estate.

CRS
Certified Residential Specialist

Learn more at www.crs.com
or call 800-462-8841.

Hotline Questions and Answers – Identity Theft Issues in Real Estate

The buyer is uncomfortable giving his SSN on the offer. He is concerned about the ID theft problem, given the number of people who will eventually have access to the offer. Is the buyer obligated to provide this information on the offer?

No. The blanks to insert the parties' SSNs have been included in the offer to assist the persons who will be preparing the transfer return for the closing. While the parties will be required to provide this information no later than closing in order to complete the transfer return, they are not required to provide the information in the offer. One possible alternative may be to provide the number in the confidential information area of the agency disclosure, with direction that it can be provided to the person preparing the transfer return. Assuming that the party refuses to provide the number until it is absolutely necessary, a strong reminder prior to closing to have the buyer bring the SSN to the closing may be helpful.

How long are we required to retain listing contracts and closing information? Also, because of ID theft, are we permitted to black out SSNs on contracts and transfer returns?

The Department of Regulation and Licensing (DRL) requires broker retention of real estate transaction records for a minimum of three years, running from the date of closing or, if the transaction didn't close, from the date of the listing contract. It may be prudent, however, to retain these records for six years in case of tax audits or litigation relating to the transaction.

Wis. Admin. Code § RL 15.04 requires "exact and complete" copies, so in spite of the broker's concerns about burglaries and ID theft, the SSNs should be left on the documents.

At a recent continuing education class, the instructor indicated that licensees no longer should have buyers and sellers put their SSNs on any of our transactional forms due to the high incidence of ID theft. The instructor said the parties should provide their SSNs to the title company, but not to put SSNs on listings and offer forms. Is that the current recommendation of the WRA?

Due to the increasing problem of ID theft, the WRA recommends that the word "confidential" be written in the area where the state-approved forms request an individual's SSN. REALTORS® should advise clients that SSNs should only be given to those persons who need them to complete the transaction. This would include, but is not limited to, the lender and title company or closing agent.

An agent transferred from one company to another. The agent's former broker is still using the agent's e-mail account with the agent's name. What privacy issues are involved and how can this be stopped?

The agent may review the former broker's office policy to determine if there is any guidance regarding the use of e-mail accounts after an agent has left the company. If the policy is silent, the agent and former broker may try to reach an agreement to either forward the e-mail messages intended for the agent to his new e-mail address or to terminate the agent's former e-mail account. If the agent and broker are unable to find a solution, the agent may wish to engage private legal counsel to look for other answers in the evolving body of law applicable to Internet issues.

Wis. Stat. § 995.50 provides for a limited right to privacy. It is an invasion of privacy to use, in advertising or for trade purposes, the name, portrait or picture of any living person without having obtained the person's written consent. It is unclear whether the e-

mail account would be deemed advertising. The agent may contact the former broker and request the broker to stop using the agent's name or image, to whatever extent that is applicable.

The federal Electronic Communications Privacy Act (ECPA) addresses privacy rights and the use and monitoring of e-mail and Internet activity. Originally adopted to regulate government activity, the Act has been used in certain employment relationships. Whether the Act would provide any recourse in this instance would require an evaluation by private legal counsel.

Are stores and other businesses allowed to print my entire credit card number on my receipt?

Beginning December 5, 2006, companies must not print credit or debit card expiration dates or more than the last five digits of your card number on your electronic receipt. Some businesses must make this change sooner, depending on the way they process credit card transactions. The law will allow receipts that are hand written or mechanically imprinted, however, to show the entire number and expiration date, even after December 5, 2006.

A broker displays an array of testimonials from prior clients and customers on his Web site. In some cases, the names of agents who are no longer with the broker's company are mentioned. Does the broker have any obligation to remove these from the Web site?

Wis. Stat. § 995.50 provides for a right to privacy. It is an invasion of privacy to use the name, portrait or picture of any living person for advertising or trade purposes, without having obtained written consent of the person. The broker may wish to stop using the names and pictures of agents unless he has their written consent. If the broker has questions, he may want to consult with an attorney.

ID Theft Resources

The “Deter, Detect, Defend” campaign is a joint project between NAR and the FTC to promote ID theft awareness to REALTORS®. The ID theft Web site is a one-stop resource to learn about the crime of ID theft. It provides a wealth of detailed information to help consumers and businesses deter, detect and defend against ID theft: www.consumer.gov/idtheft. Many of the same materials may also be found on the NAR Web site at www.realtor.org/government/affairs/identity_theft/index.html.

NAR’s Field Guide to ID Theft is available at www.realtor.org/libweb.nsf/pages/fg909.

OnGuard Online provides practical tips from the federal government and the technology industry to help consumers be on guard against Internet fraud, secure their computers and protect their personal information. Visit onguardonline.gov/index.html.

REALTORS® and consumers can test their knowledge about ID theft at www.onguardonline.gov/quiz.

The Wisconsin Office of Privacy Protection includes information about ID theft, alerts about compromised information, an extensive library of fact sheets pertaining to various aspects of ID theft, including one in Hmong, forms and guidance for filing an ID theft complaint, an

overview of the various state and federal privacy laws, press releases and other resource material at privacy.wi.gov. For more information, call the Wisconsin Office of Privacy Protection at 1-800-422-7128 or e-mail at WisconsinPrivacy@datcp.state.wi.us.

The WRA Office Policy Manual is designed to help brokers write and update their office policy manuals — to cover privacy and ID theft prevention, among other things. It covers basic office policies and procedures such as advertising, commissions, Internet usage, lead paint disclosures, computer technology and much more. To order this manual, go to www.wra.org/Products/index.asp and search for PUB239.

Upcoming Continuing Education Classes

This marks the second half of the biennium — don’t put off getting your required CE credits completed. Pick four three-hour courses included in the WRA’s 2005-2006 curriculum to satisfy the Department of Regulation and Licensing requirement. The WRA offers several state-approved continuing education courses in your area. For more details and registration information, visit www.wra.org/Cccourse or call the number listed.

October 5, 2005-2006 CE 1 & 2, 9:00 a.m. – 5:00 p.m., Brookfield

October 5, 2005-2006 CE 1 & 2, 9:00 a.m. – 5:00 p.m., Wisconsin Dells

October 5, 2005-2006 CE 1 & 2 (video), 9:00 a.m. – 4:30 p.m., Woodruff, 715-356-3400

October 5, 2005-2006 CE 4B (video), 9:00 a.m. – 12:30 p.m., La Crosse, 608-785-7744

October 6, 2005-2006 CE 3 & 4B, 9:00 a.m. – 4:30 p.m., Elkhorn, 262-723-6851

October 6, 2005-2006 CE 3 & 4B (video), 9:00 a.m. – 4:30 p.m., Woodruff, 715-356-3400

October 6, 2005-2006 CE 2 (video), 1:00 p.m. – 4:00 p.m., Kenosha, 262-942-0592

October 9, 2005-2006 CE 2 (video), 5:30 p.m. – 9:00 p.m., Two Rivers, 920-553-6227

October 9, 2005-2006 CE 3 (video), 9:00 a.m. – 12:30 p.m., Kenosha, 262-942-0592

October 10, 2005-2006 CE 4B (video), 1:00 p.m. – 4:00 p.m., Kenosha, 262-942-0592

October 10, 2005-2006 CE 3 & 4B, 8:30 a.m. – 4:30 p.m., Appleton, 920-739-9108

October 10, 2005-2006 CE 2 (video), 9:00 a.m. – 12:30 p.m., Two Rivers, 920-553-6227

October 11, 2005-2006 CE 3 (video), 12:30 p.m. – 4:00 p.m., Sheboygan, 920-457-7908

October 11, 2005-2006 CE 1 & 2, 9:00 a.m. – 5:00 p.m., Madison

October 11, 2005-2006 CE 1 & 2, 9:00 a.m. – 5:00 p.m., Milwaukee N. Port Wash Rd.

October 12, 2005-2006 CE 3 & 4B, 9:00 a.m. – 5:00 p.m., Brookfield

October 12, 2005-2006 CE 1 & 2, 8:30 a.m. – 4:30 p.m., Hudson, 651-772-6342

October 12, 2005-2006 CE 3 & 4B, 9:00 a.m. – 5:00 p.m., Wisconsin Dells

October 12, 2005-2006 CE 1 & 2 (video), 9:00 a.m. – 4:30 p.m., Woodruff, 715-356-3400

October 13, 2005-2006 CE1 (video), 9:00 a.m. – 12:30 p.m., La Crosse, 608-785-7744

October 13, 2005-2006 CE 3 & 4B (video), 9:00 a.m. – 4:30 p.m., Woodruff, 715-356-3400

October 13, 2005-2006 CE 3 & 4B, 8:30 a.m. – 4:30 p.m., Hudson, 651-772-6342

October 16, 2005-2006 CE 3 (video), 5:30 p.m. – 9 p.m., Two Rivers, 920-553-6227

October 16, 2005-2006 CE 1 & 2 (video), 9:00 a.m. – 4:30 p.m., Woodruff, 715-356-3400

October 17, 2005-2006 CE 2 (video), 9:00 a.m. – 12:30 p.m., La Crosse, 608-785-7744

October 17, 2005-2006 CE 3 & 4B (video), 9:00 a.m. – 4:30 p.m., Woodruff, 715-356-3400

October 17, 2005-2006 CE 3 (video), 9:00 a.m. – 12:30 p.m., Two Rivers, 920-553-6227

October 17, 2005-2006 CE 1 & 2, 8:30 a.m. – 5:00 p.m., Rice Lake 877-644-2265

October 17, 2005-2006 CE 3 & 4B, 8:30 a.m. – 4:30 p.m., Green Bay, 920-739-9108

October 18, 2005-2006 CE 2 (video), 9:00 a.m. – 12:30 p.m., Kenosha, 262-942-0592

October 18, 2005-2006 CE 2 & 1, 8:00 a.m. – 4:00 p.m., Campbellsport

October 18, 2005-2006 CE 3 & 4B, 8:30 a.m. – 5:00 p.m., Rice Lake, 877-644-2265

October 18, 2005-2006 CE 3 & 4B, 9:00 a.m. – 5:00 p.m., Madison

October 18, 2005-2006 CE 1 & 2, 8:30 a.m. – 4:30 p.m., Richfield, 262-338-8114 or 262-375-4730

October 18, 2005-2006 CE 4C (commercial), 9:00 a.m. – 12:30 p.m., Madison, 608-772-0060

October 19, 2005-2006 CE 1 (video), 1:00 p.m. – 4:00 p.m., Kenosha, 262-942-0592

October 19, 2005-2006 CE 3 & 4B, 9:00 a.m. – 5:00 p.m., Milwaukee S. Howell

October 23, 2005-2006 CE 4B (video), 5:30 p.m. – 9:00 p.m., Two Rivers, 920-553-6227

October 24, 2005-2006 CE 4B (video), 9:00 a.m. – 12:30 p.m., Two Rivers, 920-553-6227

October 24, 2005-2006 CE 4B (video), 9:00 a.m. – 12:30 p.m., Kenosha, 262-942-0592

October 25, 2005-2006 CE 3 & 4B, 8:30 a.m. – 4:30 p.m., Richfield, 262-338-8114 or 262-375-4730

October 25, 2005-2006 CE 3 & 4B, 9:00 a.m. – 5:00 p.m., Milwaukee N. Port Wash Rd

October 26, 2005-2006 CE 3 (video), 1:00 p.m. – 4:00 p.m., Kenosha, 262-942-0592

October 26, 2005-2006 CE 4B (video), 12:30 p.m. – 4:00 p.m., Sheboygan, 920-457-7908

October 26, 2005-2006 CE 3 (video), 9:00 a.m. – 12:30 p.m., La Crosse, 608-785-7744

October 30, 2005-2006 CE 1 & 2, 9:00 a.m. – 4:30 p.m., Rhinelander, 715-356-3400

October 31, 2005-2006 CE 3 & 4B, 9:00 a.m. – 4:30 p.m., Rhinelander, 715-356-3400

November 1, 2005-2006 CE 2 & 1, 9:00 a.m. – 5:00 p.m., Madison

November 1, 2005-2006 CE1 & 2, 9:00 a.m.– 5:00 p.m., Milwaukee N Port Wash Road

November 1, 2005-2006 CE1(video), 6:00 p.m. – 9:30 p.m., Two Rivers, 920-553-6227

November 2, 2005-2006 CE3 &4B, 9:00 a.m. – 5:00 p.m., Milwaukee N Port Wash Road

November 2, 2005-2006 CE1 & 2, 8:30 a.m. – 4:30 p.m., Appleton, (920) 739-9108

November 3, 2005-2006 CE4B (video), 9:00 a.m. – 12:30 a.m., La Crosse, 608-785-7744

November 4, 2005-2006 CE1 & 2 (video), 9:00 a.m. – 4:30 p.m., Manitowoc, 920-553-6227

November 6, 2005-2006 CE4B(video), 9:00 a.m. – 12:30 p.m., Manitowoc, 920-553-6227

November 6, 2005-2006 CE 1 & 2 (video), 9:00 a.m. – 4:30 p.m., Woodruff, (715) 356-3400

November 7, 2005-2006 CE3 (video), 9:00 a.m. – 12:30 p.m., Manitowoc, 920-553-6227

November 7, 2005-2006 CE 3 & 4B (video), 9:00 a.m. – 4:30 p.m., Woodruff, (715) 356-3400

November 7, 2005-2006 CE1 (video), 9:00 a.m. – 12:30 p.m., La Crosse, 608-785-7744

November 8, 2005-2006 CE2 (video), 6:00 p.m. – 9:30 pm, Manitowoc, 920-553-6227

November 8, 2005-2006 CE1 & 2, 8:30 a.m. – 4:30 p.m., Janesville, (608) 755-4854

November 8, 2005-2006 CE1 & 2, 8:30 a.m. – 4:30 p.m., West Bend, 262-338-8114

November 8, 2005-2006 CE1 & 2, 9:00 a.m. – 4:00 p.m., Sheboygan, 920-457-7908

November 9, 2005-2006 CE 2 & 1, 9:00 a.m. – 5:00 p.m., Brookfield

November 9, 2005-2006 CE3 & 4B, 8:30 a.m. – 4:30 p.m., Janesville, (608) 755-4854

November 9, 2005-2006 CE 3 & 4B, 9:00 a.m. – 5 p.m., Madison

Protect Yourself With Pearl

*Comprehensive E&O coverage
with a personal touch*



**WISCONSIN
REALTORS®
ASSOCIATION**

(Sponsored since 1994)

P E A R L
INSURANCE

1.800.289.8170

www.pearlxdate.com