



ARE YOU IN COMPLIANCE WITH RECENT IDENTITY THEFT REGULATIONS?

By Barry S. Goodman, Esq.

This article appeared in the August 2005 issue of New Jersey REALTOR® magazine.

Have you ever taken a social security number on a sales contract to prequalify a buyer or as part of a lease application? How about driver's license numbers? Credit or debit card information? Bank account numbers? Under recently enacted federal and State laws, such information now is regulated for all businesses, including real estate brokers. As a result, if you ever take such personal information, you must be aware of your legal obligations for the proper disposal of the information and what you have to do if there ever is an unauthorized access to the information. You also will have to carefully safeguard the use of Social Security Numbers ("SSNs").

Background

As we all know, identity theft is becoming a major problem. Victims can have their good names and credit ruined and spend years trying to repair the damage that was done to their credit histories.

As a result, on the federal level, the Fair and Accurate Credit Transactions Act of 2003 ("FACTA") was passed empowering the Federal Trade Commission ("FTC") to promulgate rules concerning the proper disposal of personal financial information. As a result, the FTC has created the "Disposal Rule," which became effective on June 1, 2005.

Similarly, the New Jersey Legislature now has passed the Identity Theft Prevention Act, which will become effective January 1, 2006.¹ This Act not only deals with the disposal of personal financial information but also imposes notice requirements if there is a breach of security and sets forth specific restrictions on the use of SSNs.²

Disposal of Consumer Credit Information

Under the federal Disposal Rule, any person or entity, which would include a real estate broker, who maintains or possesses information taken from consumer reports for a business purpose must properly dispose of such information. A broker therefore cannot simply throw documents, disks or other material containing personal credit information into the garbage.

The FTC, while acknowledging that there is no such thing as "perfect destruction," has required that businesses must take "reasonable measures" when disposing of consumer information. Examples that the FTC has provided of proper disposal include (1) burning, pulverizing or shredding papers; (2) deleting or erasing electronic media; and (3) using document disposal companies.

New Jersey's Identity Theft Prevention Act follows the federal Disposal Rule but adds some wrinkles. The Act defines acceptable means of destruction as including "shredding, erasing or otherwise modifying the personal information in those records to make it unreadable, undecipherable or nonreconstructable through generally available means," which essentially follows the federal requirements. However, New Jersey has expanded the definition of what consumer information must be properly destroyed once the record no longer is needed. Such personal consumer information includes any records that contain an individual's first name (or first initial) and last name linked with any one or more of the following:

1. social security number;
2. driver's license number or State identification number; or

3. account number or credit or debit card number in combination with any required security code, access code or password that would permit access to an individual's financial account.

Thus, in order to comply with both federal and State law, all records, including electronic and hard copies, must be destroyed in a manner that would prevent an unauthorized person's access to them. Hard copies of documents can be shredded and computerized records must be deleted when they no longer are needed or required by law to be kept if they contain such personal information. Failure to comply with these disposal requirements can, under the federal law, result in significant fines and potential civil liability to consumers who have been harmed.

Notification Requirements

The New Jersey legislation also outlines procedures that businesses, including brokers, who compile or maintain computerized records that include personal information must follow when the broker discovers or is made aware of the unauthorized access of a client's or customer's personal information. First, the broker must report this breach of security to the State Police without delay. Unless a law enforcement agency requests otherwise, the broker then must expeditiously contact the customers or clients whose information may have been accessed. Disclosure is not required, however, if the broker establishes that "misuse of the information is not reasonably possible."

If the broker compiles or maintains computerized records that contain personal information on behalf of another business or entity, the broker must notify that business of the breach. Statutory language is unclear with regard to whether the broker or the other business must contact the State Police. Therefore, to be safe, a broker should contact the authorities immediately upon the discovery of the breach. The other business will be responsible for contacting and disclosing the breach to the clients or customers.

Notification of clients and customers can be provided in several ways. First, a broker can provide written notice of the breach. Next, notification may be given electronically.³ However, if the notice would cost more than \$250,000 or would have to be given to more than 500,000 people, a substitute form of notice will be sufficient. Substitute forms include e-mail notice, readily apparent and accessible notice on the broker's website and notice to Statewide media. Finally, if notice has to be given to more than 1,000 people, the broker also must modify all nationwide consumer reporting agencies. Such notification must include the details regarding the "timing, distribution and content of the notices" to those persons whose information was accessed.

Use of Social Security Numbers


The New Jersey legislation also strictly regulates the use of an individual's SSN. A broker may not post or publicly display four or more consecutive numbers of an individual's SSN, print an individual's SSN on any mailed materials (unless required to do so by State or federal law), or intentionally communicate or otherwise make available a person's SSN to the general public. It also is illegal to require individuals to provide a SSN on the Internet "unless the connection is secure" or the "number is encrypted." Furthermore, a business may not require individuals to use their SSNs to gain access to a website, unless additional information also is necessary.

Although the legislation greatly restricts the use of SSNs, it permits the use of SSNs when they are required by state or federal law for "Internet verification and administrative purposes." SSNs also "may be included in applications and forms sent by mail, including documents sent as a part of an application or enrollment process, or to establish, amend or terminate an account, contract or policy, or to confirm the accuracy" of the SSN. However, even in applications and other forms, SSNs may not appear on the outside of envelopes, postcards, mailers without envelopes or where they can be seen through an envelope.

Conclusion

It therefore is important for real estate brokers to comply with these federal and State requirements. Brokers should be sure to completely destroy all documents and computerized records that contain a customer's or client's personal information when disposing of such materials.

Measures also obviously must be taken to avoid access to such personal information by unauthorized individuals. However, if a broker discovers that such information has been accessed by an unauthorized person, the broker



immediately must contact the State Police. The broker then also must notify the customer or, if the information was maintained or compiled for another entity, the other entity.

Finally, since the use of SSNs has been severely restricted, brokers must be careful not to misuse SSNs. SSNs should be kept secure and disposed of according to the federal and State requirements.

Endnotes

1. This legislation was waiting for the Acting Governor's signature as this article was written. It is expected that this legislation will have been signed by the Acting Governor by the time this article is published.
2. The new legislation also provides, among other things, the procedures for a consumer to place a security freeze on his or her consumer report that only is applicable with regard to consumer reporting agencies.
3. Any electronic notice must be consistent with the provisions regarding electronic records and signatures in the federal Electronic Signatures in Global and National Commerce Act. 15 U.S.C. § 7001, et seq.