Pennsylvania Association of REALTORS®

The Voice for Real Estate® in Pennsylvania

A BROKER'S GUIDE TO CONSUMER DATA SECURITY AND CONFIDENTIALITY

I. OVERVIEW OF APPLICABLE LAWS

The confidentiality and security of information obtained by a real estate brokerage is regulated and governed by several federal and state laws as well as the National Association of REALTORS® (NAR) Code of Ethics (Code). This guide will provide brokers with a detailed overview of the applicable laws and the Code including the requirements, prohibitions and applicability of each, followed by recommendations for applying the laws and the Code together in areas where data and information security concerns are likely to exist or arise in a brokerage.

The Real Estate Licensing and Registration Act (RELRA) and the Code

The RELRA and the Code contain nearly identical provisions regarding the confidentiality of client information. Although the type of information that must be kept confidential is not clearly defined in either RELRA or the Code, a functional definition of confidential client information implicitly protected by these provisions is as follows:

> "Any non-public information obtained for, by or in regards to a current or former client of a real estate licensee and/or brokerage during the course of an agency relationship, which could be used by the licensee or a third party to the current or future detriment of the client."

This confidential information is required to be treated as follows:

> "A brokerage and its affiliated licensees shall not knowingly, during or following the termination of an agency relationship, reveal confidential client information (including confidential information from former clients) or use such confidential information to the advantage of a licensee or a third party except when the disclosure or use is made:
>
> a. with the consent of the client;
> b. solely to another licensee or third party acting on behalf of the client and not for another party;
> c. as required by law;
> d. it is the intention of the client to commit a crime and the disclosure is believed necessary to prevent the crime; or
> e. the information is used to defend the licensee or brokerage in a legal proceeding against an accusation of wrongful conduct."

Additionally RELRA imposes general duties on all licensees to act in the best interests of their clients, which would presumably include reasonably safeguarding any otherwise private information of the client received by a licensee such as financial account numbers and individual

identification information like social security numbers. Violation of RELRA may subject a licensee and/or brokerage to the full range of possible licensing sanctions including public reprimands, civil monetary penalties and possibly real estate license suspension or revocation.

The Privacy of Social Security Numbers Act (PSSNA)

The PSSNA is a Pennsylvania statute that governs the acquisition, protection and use by businesses, including real estate brokerages, of consumer social security numbers (SSNs). The application of the PSSNA is not limited to a broker's clients, but applies to the SSN of any consumer who comes into contact with the brokerage and also applies in a human resources context to employees and agents of the brokerage. The PSSNA prohibits the following:

1. Printing an individual's SSN on any card required to access products or services provided by the person or entity.
2. Requiring an individual to transmit their SSN over the Internet unless the connection is secure or the SSN is encrypted.
3. Requiring an individual to use their SSN to access an Internet website unless a password or unique access personal identification number or other authenticating device is also required.
4. Printing an individual's SSN on any material mailed to that party unless Federal or State law requires the SSN to be on the document mailed, in which case the printed SSN may not be mailed in a form where the SSN can be seen prior to opening an envelope.
5. Intentionally posting or displaying an individual's SSN to the public.

The PSSNA does not prevent collection or use of an individual's SSN where the use is required by law or for legitimate internal verification or administrative purposes. Some legitimate purposes fitting into these categories for a real estate brokerage would include:

1. Performing a domestic relations lien search;
2. Running a credit report;
3. Filling out a W-9 to open an interest-bearing escrow account; and
4. Verifying that a seller is not a foreign entity for the purposes of compliance with the federal Foreign Investment in Real Property Act – FIRPTA – (mostly for commercial transactions).
5. Uses of agent/employee (including applicants for employment and prospective agents) SSNs for reporting income and withholding tax, performing background checks and other legitimate Human Resource related functions.

The PSSNA also allows the continued use of SSNs in manners that are inconsistent with the general prohibitions of the Act if the use pre-dated the Act, but it is strongly recommended that all brokerages discontinues such practices and only collect, store and use SSNs as allowed under the PSSNA. Fines for violating the PSSNA range from $50 - $500 for the first offense, and $500 - $5000 for any subsequent offense. In addition, local district attorneys and the State Attorney General are given authority to institute criminal proceedings for violations under the PSSNA.

The Breach of Personal Information Notification Act (BPINA)

The BPINA is a Pennsylvania consumer notification law that has implications for consumer data security. The BPINA requires businesses, including real estate brokerages, who maintain consumer "personal information" of Pennsylvania residents to notify those consumers when there has been a breach of the computerized data security system in which the information is stored. The BPINA defines "personal information" covered by this law as:

> An individual's first name or first initial and last name in combination with and linked to the individual's:
>
> 1. Social Security Number
> 2. Driver's license number or a state identification card issued in lieu of a driver's license
> 3. Financial account number, 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.

The BPINA applies only to computerized data containing such "personal information" and contains exceptions for redacted and/or encrypted data. Redaction under the BPINA requires that the listed data elements stored in the database contain no more than the last four digits of the social security number, driver's license/state identification card or account number. If the data is *stored and accessible* only in redacted form (i.e., the database contains no more than the last four digits, not that the others are in the system but blacked out to a user), then the BPINA does not apply to that data.

The technical definition of encryption is "an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key." In short, encryption is a process that scrambles data unless the user has a password or other "key" that unscrambles the data to make it useful. Encryption, unlike redaction, is not a complete exemption from the BPINA because encrypted data which is lost or stolen might still be misused if the breach of security involves someone who has also stolen the key (or who already had it). For this reason, the BPINA does not exempt encrypted information when:

1. the encrypted information is accessed in an unencrypted form;
2. the security breach is linked to a breach of the security of the encryption key; or
3. the security breach involves a person with access to the encryption key.

Note that there is no definition of the term "computerized data" within the law. To be prudent, it must be assumed that the definition is as broad as possible to cover all sorts of storage methods that might be considered "computerized." In addition to a typical database application, this term likely also includes: CRM or other marketing software; e-mails; faxes or voicemails received via computer or that have been converted to electronic format for e-mail delivery; text messages; and any other data that is stored on your desktop computer, laptop computer, cell phone, Blackberry, Treo or other handheld device in any way.

The notification requirements of the BPINA are triggered when:

1. there has been a breach of the security of the computerized data system containing the personal information of a resident of Pennsylvania;
2. the entity reasonably believes that the information has been accessed and acquired by an unauthorized person.; and
3. the entity reasonably believes that the compromised security of the system has caused or will cause loss or injury to a resident of Pennsylvania.

Since it is virtually impossible to know how compromised person information will be used by the unauthorized person who acquires it, a brokerage should almost always presume that a security breach will cause loss or injury to the individuals whose information has been accessed.

Remember that computerized data covers virtually any data stored in an electronic fashion, so the definition of a "breach" of that security may be very broad. For example, losing a hand-held data device (a Treo or Blackberry, for instance) would be considered a security breach. Proof of unauthorized access to a desktop or laptop computer would probably be considered a security breach as well, as it is possible that another person might have accessed the secure information.

Notification must be made without unreasonable delay after determining the scope of the breach and integrity of the data system has been restored. There are four primary ways to provide notice to a consumer in the event of a breach or a suspected breach. Notification may be made by *any* of the methods.

1. Written notice to the last known home address.
2. Telephonic notice if there is a reasonable belief the consumer will receive it and only when the notice is given in a "clear and conspicuous manner." Clear and conspicuous manner is a message that describes the incident in general terms. However, when using this method, the resident must not be required to provide personal information, but is instead should be given a telephone number to call or Internet website to visit for further information or assistance.
3. Email notice is allowed when there is a prior business relationship and a valid email exists for the consumer.
4. Substitute notice is allowable when the cost of providing notice exceeds $100,000 or the breach affects number of consumers exceeds 175,000 or the entity does not have sufficient contact information to make notification. Substitute notice may be by any of the following methods:
    a. Email notice if an email address exists for the resident; or
    b. Conspicuous posting of notice on the entity's website, or
    c. Notification via a major statewide media.

The brokerage must also make a report to all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis whenever a breach of data security affects more than 1,000 Pennsylvania residents. This notification must also be made without unreasonable delay.

The BPINA also applies to third party vendors who store, maintain, manage and/or destroy computerized data containing "personal information" on behalf of a brokerage. This notification

requirement only requires the vendor to notify the business entity from which it received the breached data of the existence and extent of the breach; the entity that was collecting the information still has the responsibility to notify all of the affected consumers directly. For example, if you store customer information online through a third-party contact management system and that company has a security breach, it is their responsibility to notify you, and your responsibility to notify all of the consumers whose information you were storing.

A violation of the BPINA is considered to be an unfair and deceptive trade practice in violation of Pennsylvania's Unfair Trade Practices and Consumer Protection Law ("UTPCPL"). The BPINA exclusively authorizes the Pennsylvania Attorney General to bring civil actions under the UTPCPL. Penalties can range from a statutory minimum of $100.00 per violation to triple the amount of actual damages suffered by a consumer.

The Fair Credit Reporting Act (FCRA)

The FCRA is a federal statute enforced by the Federal Trade Commission (FTC). In 2003, Congress passed the Fair and Accurate Credit Transaction Act (FACTA), which modified the FCRA in an effort to combat the increasing problem of identity theft. The FTC subsequently promulgated regulations to put the FACTA modifications into effect. The law and accompanying regulations require that certain consumer information received by businesses, including real estate brokerages, be disposed of in a secure manner.

The information covered by these regulations is limited to "consumer information" in the form of a "consumer report" or information derived from the data in a consumer report. Consumer reports, frequently called credit reports, are reports on a person's credit history/worthiness, employment history and/or reputation, compiled by a consumer reporting (i.e. credit) agency. In the brokerage field such information may be found directly in credit reports acquired as part of a tenant or buyer screening process and indirectly in the form of a mortgage pre-qualification, commitment or denial letter.

Although the regulations do not specifically state how this "consumer information" should be disposed of, it strongly implies that shredding or any other method which ensures that the information is permanently destroyed or otherwise made permanently inaccessible is sufficiently secure. The regulations allow for the disposal to be carried out by third party vendors, but require the business that originally held the "consumer information" must ensure that the third party vendor disposes of it securely. Violations of the FCRA and/or its regulations can result in civil penalties of $1,000.00 per offense, plus any actual consumer financial loss and payment of the prevailing party's attorney fees and court costs.

General Consumer Protection Laws

The Federal Trade Commission Act (FTCA) and Pennsylvania's Unfair Trade Practices and Consumer Protection Law (UTPCPL) are general consumer protection laws. The FTCA is the tool currently being used by the federal government to force large monetary settlements from businesses around the country based on their improper disclosure of consumer financial information. Pennsylvania's UTPCPL is similar in nature and structure to the FTCA and is often used as a guide for Pennsylvania courts presented with cases of first impression involving the UTPCPL. The FTCA is enforced by the Federal Trade Commission (FTC), while the UTPCPL

is enforced by the Pennsylvania Office of Attorney General (AG). Both laws also allow for a private cause of action to be brought in the civil court system. The UTPCPL is not being widely used to bring such claims at the state level, but a violation of the FTCA is considered a violation of the UTPCPL in Pennsylvania.

Neither the FTCA nor the UTPCPL contains any language specifically pertaining to the security or disclosure of financial information. The federal cases are being brought under section 45 of the FTCA that simply prohibits unfair or misleading trade practices. A similar "catch-all" provision is contained in the UTPCPL. The federal claims that have been brought are based on unfair trade practices where the accused businesses either failed to adhere to their own consumer privacy policies and notices and/or simply failed to take "reasonable" steps to secure the consumer financial information they possessed. Claims under both laws can result in civil lawsuits seeking statutory or actual damages (possibly including triple damages), attorney fees and court costs.

II. PRACTICAL GUIDANCE ON BROKERAGE DATA SECURITY

Employee and Licensee Activities

Every brokerage should have in place a policy specifically guiding the actions of any brokerage employee or affiliated licensee who receives, requests, uses, maintains, stores or discards any consumer information that is protected by the laws noted above. The policy should contain specific prohibited activities, legal requirements and guidelines for handling such information. The policy should be written to be understood at the employee/licensee level and should seamlessly incorporate the various laws into a single set of rules and guidelines. PAR has a sample data security and confidentiality office policy available for use and adaptation by its members. Brokerage counsel should review the policy to ensure that it covers all activities carried on by the brokerage.

Employees and licensees should also receive regular training and education regarding consumer information and data security. In-house training, formal seminars and the use of various forms of educational media can be very effective methods for enforcing the reasons underlying the brokerage data security policy.

Vendor Contracts

Most brokerages use one or more third party vendors to handle their consumer information and data that may be protected by law. A small sampling of such vendors includes, but is certainly not limited to:

1. Electronic standard form vendors.
2. Website hosting vendors.
3. Record storage companies.
4. Database management companies.
5. Record/data disposal companies.

Contracts between brokerages or individual licensees and vendors who will receive protected consumer information of any kind from the brokerage and/or licensee should contain the following provisions at a minimum:

1. Compliance – The vendor should agree to comply with all current and future applicable federal and state laws and the brokerage's policy on consumer data and information security and confidentiality. The list of applicable laws, especially Pennsylvania specific laws, should be identified, but should not be considered all inclusive. A copy of the brokerage policy should be provided to the vendor as part of this provision. The contract should require the vendor to list any third parties to which it may forward some or all of the data, should require that the vendor receive the same or greater assurances of compliance from any vendor it uses and should state that the vendor who signs the contract remains ultimately responsible for all data and information it receives from the brokerage.
2. Audits and Inspections – Depending on the function performed by the vendor, the contract should allow the brokerage to audit and/or inspect the vendor's facilities, security protocols and practices, records and/or policies as needed to ensure that the compliance promises made by the vendor are valid and consistently performed. The contract should address the depth, type, and frequency of audits and inspections.
3. Notification – The contract should require the vendor to timely notify the brokerage each time any compliance provisions of the contract, applicable laws or the brokerage policy is breached or violated. The manner, timing, form and extent of notification should all be addressed in the contract.
4. Indemnification – The contract should require the vendor to indemnify the brokerage for any loss, breach or other unauthorized access or disclosure of consumer information provided to it by the brokerage caused by the acts or omissions of the vendor, its agents, employees and any third party vendors it uses. The indemnification should specifically cover all costs associated with the security breach including, but not limited to costs of making any required consumer, governmental or other entity notifications, costs of any compensatory damages paid to any consumer or other entity, including all attorney fees and costs, and any other related, consequential financial losses.

Vendor contracts may or may not be negotiable on these points. Qualified legal counsel should be consulted to review the contracts as needed. In-house or contracted data security professionals should be consulted to ensure that the security claims represented by the vendor in the contract negotiation process are in accordance with current standards and practices within the data security industry.

It is important to remember that the broker is ultimately responsible for the activities of all affiliated licensees and employees. This responsibility extends to compliance issues, including compliance with these laws. As such, all affiliated licensees of the brokerage should be required to have any contracts between themselves and any third party vendor who may come into contact with protected consumer information/data reviewed and approved in advance by their supervising broker.

Brokerage Security of Consumer Information and Data

Each brokerage should review its current practices to determine how best to ensure compliance with all consumer information confidentiality and security laws. An internal audit should be performed to determine in detail when and how potentially protected consumer information is requested, acquired, used, stored, maintained and disposed of. Adequate security measures and/or policies and procedures should then be put into place to ensure the security of that information.

The following are general methods used to reduce the potential liability of a brokerage suffering a consumer information/data breach:

1. Minimization – After determining where and when protected consumer information is acquired by the brokerage, the next step should be to determine how the acquisition of such information can be reduced. Each brokerage should find and eliminate any unnecessary intake, use or retention/storage of protected consumer information. Valid and necessary uses of such information should not be targeted, but the value of each use should be analyzed to determine what information is needed and what information is either completely unnecessary or can be directed to other parties who truly need the information. A brokerage cannot lose or disclose information that it never receives.
2. Physical Security – Each place where protected consumer information is found should be protected by common sense physical security. Locked drawers and file cabinets, secure briefcases, building and automobile security systems are obvious needs. Placing fax machines and printers in secure areas and ensuring privacy of conversations is also important. Physical security measure can even be incorporated into electronic devices with laptop cable locks.
3. Electronic Security – Security of brokerage-wide and individual electronic devices such as desktop and laptop computers, computer networks and servers, PDAs and even cell phones is a critical component of data security. Encryption and/or redaction of data at the database level, the use of adequately secure computer passwords, hardware and software firewalls, anti-virus/anti-spyware programs and other electronic security devices are primary lines of defense. Data security standards and techniques are constantly evolving as the threats to data continue to evolve. A competent computer security professional should be engaged to ensure that a brokerage's computerized devices are protected by up to date security technology.
4. Culture of Security - A computer password is useless when it is posted next to a computer or saved in the computer's memory to ease access for the user. Data and information security devices and technology can only work when the end users, licensees and employees of the brokerage, consistently and consciously adhere to a data and information security mind set.

Record and Device Disposal

Improper disposal of consumer information and data can violate every law discussed above. Records of real estate files are usually discarded in batches, and as such a single episode of improper record disposal will likely compromise the protected information of many individuals. In-house or contracted shredding and/or pulverizing of paper documents and tangible electronic storage media such as computer discs and thumb drives is highly recommended. Adequate tracking of records will ensure that all records will be destroyed in a timely manner. Throwing records into the trash is a recipe for disaster.

Records should only be destroyed after their proper retention period has passed. Ensure that you discuss with brokerage counsel and your accountant how long various sorts of business records should be retained (remember that these laws apply to employee information just as they do to consumer information). Be sure to communicate and enforce your retention and destruction policies with all employees and licensees, as well. Where a licensee might keep a duplicate file in a home office or store electronic copies of documents off-site, it is important that the licensee destroy records on the same schedule as the broker and in a secure manner.

Disposing of electronic devices that have electronic memory capabilities is an area of great concern. The storage media with in the device should be removed and physically destroyed or rendered irreparably inoperable before the device is discarded. Simply deleting files from a computer's memory is inadequate. If a device with memory capabilities is to be sold, donated or otherwise leave the control of the brokerage or licensee without physically destroying its storage media, then care should to taken to ensure that the memory has truly been wiped clean. A computer technology professional should be consulted for the proper techniques required to do this for each device. This applies not only to desktop and laptop computers, but also to other data devices such as cell phones, Treos or Blackberries that might contain personal information of consumers. Check your user manual and customer service for the most secure method to eliminate data from these devices before handing them down or selling them to another user.

Summary

The above information is a compilation of information from various sources, including resources available on the PAR Web site at www.parealtor.org. This Broker's Guide is NOT a brokerage policy statement, although it does provide guidance on many issues that a broker would need to consider in drafting such a policy statement. Note that a sample policy is available on the Web site, although as with any PAR sample policies a broker should always seek advice from brokerage counsel on developing a policy that fits the needs of your particular brokerage.