

RECORD KEEPING AND PRIVACY REQUIREMENTS

Property managers collect and retain quite a bit of confidential information about their residents and applicants. Among other things most properties ask their residents/applicants to provide:

- Full names
- Dates of birth
- Social Security Numbers
- Recent addresses
- Driver's license numbers and/or other federally issued identification such as passports, visas, etc.
- Sources of income, including employment and disability payments
- Other credit data obtained from national credit reporting agencies.

This information is used for credit and background screening and is often retained throughout the person's tenancy, as part of the tenancy file. While this data collection is a useful tool for evaluating the creditworthiness and other characteristics of potential and current residents, it can also create pitfalls for properties that don't properly maintain and dispose of it.

Because of the extreme risk of identity theft if this confidential information is misused, Arizona and federal law impose significant responsibilities on persons and entities that acquire it. Persons and entities that fail to comply with these requirements face civil penalties and may also be liable under tort claims to the persons whose confidential information was inappropriately disclosed.

The Federal Fair Credit Reporting Act

The Federal Fair Credit Reporting Act (FCRA) regulates the dissemination of confidential credit-related information in the United States. While most of the law regulates banks and credit reporting agencies, it also creates Red Flag Rules that are applicable to any "creditor" that obtains information from a national credit-reporting agency.

"Creditors" include any businesses or organizations that regularly provide goods or services first and allow customers to pay later. The term also includes all businesses that make credit decisions about consumers affecting household related goods and services. While commercial landlords are excluded from this definition, residential landlords that use credit reports to make decisions about whether or not to rent to a particular individual, or how much of a deposit to require, are clearly covered. Because residential landlords also usually have "covered accounts," i.e. they allow the consumer to make multiple payments or transactions for the goods or services, they are required to develop and implement a written program to detect and respond to the red flags of identity theft. This program is generally referred to as a written Identity Theft Prevention Program.

The Federal Trade Commission (FTC), which administers the FCRA, strongly recommends that companies retain only that information concerning their customers for which there is a foreseeable business need. If businesses need to keep confidential personal information, then the FTC suggests that the business:

- Develop a written records retention policy to identify what information must be kept and for how long, and how to dispose of it when it is no longer needed.
- Require that files containing personally identifiable information be kept in locked file cabinets unless they are in use.
- Require employees to put all files away, log off of their computers and lock all file cabinets at the end of the day.
- Ensure all electronic data is protected with firewalls, passwords and similar security devices,

Finally the Red Flag Rules require businesses to develop a written plan on how to respond to security breaches or an incident of identity theft involving their businesses. In some circumstances this requires the property to notify national credit reporting agencies, police departments and known or potential victims of identity theft. The FTC has designed a form to help groups at low risk for identity theft put together this program. It is available at www.ftc.gov/redflagrule.

In addition to these Red Flag Rules, the FTC has developed an additional rule requiring creditors to properly dispose of confidential personal information that they obtain in the course of their business. This rule, called the Disposal Rule, requires creditors (specifically including landlords and employers) to develop disposal practices that are reasonable and appropriate to prevent the unauthorized access to, or use of, information in a consumer report. While the Disposal Rule allows creditors some flexibility as to the methods they may use to dispose of confidential information it anticipates that creditors will establish written rules and regulations for disposing of confidential consumer data and will train employees with respect to those regulations. And while the rule does not define what constitutes confidential consumer information, it assumes that such data as a person's name, social security number, driver's license number, phone number, physical address, and email address would normally be included. In addition, some data that standing alone would not identify an individual, may also be protected consumer information if it would do so if it was released in combination with other information.

Under the Disclosure Rule covered entities must take reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal." "Disposal" includes discarding or abandoning the "consumer information," as well as the sale, donation, or transfer of any medium (including computer equipment) that contains "consumer information." While the FTC recognizes that one size does not fit all situations, it generally suggests that creditors consider burning, pulverizing, or shredding papers containing

“consumer information” so that the information cannot as a practical matter be read or reconstructed. Electronic data generally should be disposed of by destroying or erasing electronic files or media containing consumer report information.

It is important to comply with these requirements. Although the FTC does not conduct routine compliance audits of businesses, it can conduct investigations to determine if a business within its jurisdiction has taken appropriate steps to develop and implement a written program as required by the rule. If the agency determines that the entity is not compliant it can seek civil penalties of \$3500.00 per violation and injunctive relief. As each instance in which the entity has failed to comply with the rule constitutes a separate violation, these penalties can become substantial.

Arizona Rules Regarding Disposal of Confidential Information

The Arizona legislature has also established penalties for improperly disposing of confidential information.

A.R.S. § 44-7601 provides that an entity “shall not knowingly discard or dispose of records or documents without redacting the information or destroying the records or documents if the records or documents contain an individual’s first and last name or first initial and last name in combination with” the person’s (a) social security number; (b) credit card, charge card, or debit card number; (c) retirement account number; (d) savings, checking or securities entitlement account number; or (e) driver license number or no operating identification license number.

In the event of violations, the entity can be sued by either a county attorney or the Arizona Attorney General and can face civil penalties for each violation arising out of one incident. Those civil penalties start at \$500 for a first violation and go up to \$5000.00 for a third or subsequent violation. A safe harbor exists if the entity has its own procedures for discarding or disposing of these records and complies with those procedures.

Arizona Law Concerning Breach of a Security System

If an Arizona business that owns or licenses unencrypted computerized data that includes personal information becomes aware that an unauthorized person has acquired access to that information, A.R.S. § 44-7501 imposes specific notice requirements on the owner of the information. Specifically it requires the owner to conduct a prompt investigation to determine if there has been a breach of the security system, and if such a breach is determined, notification to the individuals affected by the breach. That notification must be provided either:

- In writing
- Electronic notice if the person’s primary method of communication is by electronic means
- Telephonic notice, or

- Substitute notice if actual notice would cost the business more than \$50,000.00.

The law also provides that if a business maintains its own notification procedures as part of an information security policy (such as that required by the Red Flag Rule) that notification procedure provides a safe harbor under the Arizona law.

Social Security Numbers

In addition to the more general requirements, Arizona lawmakers have also strictly regulated information concerning social security numbers. A.R.S. § 44-1373 makes it unlawful for a “person or entity” to take any of the following actions:

- Intentionally communicate or otherwise make available an individual’s social security number to the general public.
- Print an individual’s social security number on any card required or the individual to receive products or services provided by the person or entity
- Require the submission of an individual’s social security number over the Internet unless the connection is secure or the social security number is encrypted.
- Require the use of an individual’s social security number of access an internet web site unless a password or unique personal identification number or other authentication device is also required to access the site.
- Print a person’s social security number on any materials that are mailed to an individual unless required by state or federal law; however, a property may mail documents that include a social security number sent as 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 social security number.
- Record documents or records that are made available to the recording entity’s public website and that contain more than five numbers that are reasonably identifiable as being a part of an individual’s social security number. These documents also may not contain an individual’s (a) credit card, charge card, or debit card numbers; (b) retirement account numbers; (c) savings, checking or securities entitlement account numbers.

Persons who violate this statute are subject to prosecution by the Arizona Attorney General or a county attorney.