

# Kimball, Tirey & St. John LLP

## “Red Flag Rules” – It’s Time to Act

*Nicole Ferree and Craig D. McMahon, Esq.*

**October, 2009**

Prompted by the nearly 10 million Americans that have fallen victim to identity theft, the Fair and Accurate Credit Transactions Act of 2003 (FACTA) amended the Fair Credit Reporting Act (FCRA) and mandated that financial institutions and creditors develop and implement a comprehensive, written identity theft program aimed to protect businesses and consumers from identity theft. The FACTA establishes new rules referred to as “Red Flags” that require financial institutions and creditors to develop policies and procedures for identifying, detecting, and responding to any practice or activity that may indicate potential identity theft. The compliance date for these Red Flag rules is November 1, 2009.

While in 1999, the Federal Trade Commission determined that the landlord-tenant relationship was not a creditor relationship under the FCRA, we are concerned that future interpretations of the legislation may broaden its scope to include property managers and owners as creditors. Prudent property managers and owners should voluntarily comply with the regulations not only to protect themselves and tenants (current, potential, and former) from the harms of identify theft but also to protect themselves from potential future civil liability.

Property managers and owners often have access to personally identifying information including names, addresses, telephone numbers, social security numbers, and income and credit histories. A successful, written identity theft program will ensure that this information is handled efficiently and securely. While FACTA provides businesses with a great deal of flexibility in developing their identity theft programs to accommodate the specific needs and potential risks that present themselves to each unique business, every plan must:

- Identify and assess relevant “red flags” in each area of operation. “Red flags” are warning signs that may indicate possible identity theft.
- Develop and implement a safeguard program to detect red flags.
- Develop an appropriate response plan for each applicable red flag to prevent and mitigate identity theft.
- Include a plan to update the program.

Before developing a written identity theft prevention program, determine what personally identifying information is currently being collected and stored, and decide whether there is a legitimate business need to do so. Minimizing the amount of unnecessary information collected reduces an unnecessary risk. Establish a time limit for retention of records consistent with your legal obligations and your business needs. Do not retain information that is unnecessary to the operation of your business after the established time period has expired. Information which you deem unnecessary should be destroyed appropriately.

Once it has been determined what information is relevant, a comprehensive identity theft prevention program will need to be devised in order to establish policies and procedures to safeguard that information. Identify red flags that may be indications of possible identity theft. These red flags may include address discrepancies, suspicious documents, or any other

unusual activity. A successful identity theft program should detail how to detect these red flags as well as how to appropriately respond to them.

There are other components of this current legislation that apply to property managers and owners. For example, the new law also requires users of consumer reports to develop reasonable policies and procedures to utilize when reviewing a notice of address discrepancy from a consumer reporting agency. Additionally, if the user reports information to a consumer reporting agency, the user must develop and implement reasonable policies and procedures for furnishing an address regarding the consumer.

An identity theft prevention program will prepare you for any future interpretations of the law which may make compliance mandatory and it makes good business sense. Individuals are more likely to do business with trusted property managers and owners who they believe will keep their information confidential and secure.

**If you are interested in obtaining legal services in order to better understand these new requirements or for assistance with the development of your written identity theft prevention program, please contact Susan Aguilar at (800) 575-1770.**

*Nicole Ferree is a graduate from the University of California at Irvine, and is currently a second year law student at the University of San Diego School of Law. She is a law clerk at Kimball, Tirey & St. John LLP in the Business Real Estate Practice Group*

*Craig D. McMahon is a partner at Kimball, Tirey & St. John LLP. Mr. McMahon consults on ADA and fair housing issues throughout California. Kimball, Tirey & St. John specializes in landlord/tenant, collections, business and real estate law, with offices throughout California.*

---

*Kimball, Tirey & St. John LLP is a full service real estate law firm representing residential and commercial property owners and managers. This article is for general information purposes only. Before acting, be sure to receive legal advice from our office. If you have questions, please contact your local KTS office. For contact information, please visit our website: [www.kts-law.com](http://www.kts-law.com). For past Legal Alerts, Questions & Answers, and Legal Articles, please consult the resource library section of our website.*