NMHC National Multi Housing Council®

National Apartment Association

TO: NMHC Members

FROM: Jim Arbury, NMHC Senior Vice President of Government Affairs
Jeanne McGlynn Delgado, NMHC Vice President of Business and Risk Management Policy

RE: FACT Act's Identity Theft Rules Effective November 1, 2008

DATE: October 22, 2008

NMHC members should be aware of new federal identity theft prevention rules that go into effect on November 1, 2008 and impose some compliance obligations on apartment firms as users of consumer credit reports. The rules were published on November 9, 2007 (72 FR 63718) by the Federal Trade Commission (FTC) to implement Sections 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003 (FACT Act).

Known commonly as the "Red Flag" and Address Discrepancy Rule, its overall objective is to prompt businesses to take additional steps to authenticate a person's identity when certain warning signs of potential ID theft are present. The first two sections of the rule outline steps that financial institutions and creditors have to take to detect and mitigate the risks of "red flags" that might signal possible identity theft. They also require credit and debit card issuers to implement procedures to assess the validity of a change of address request followed closely by a request for a new or replacement card.

While apartment firms do not, in most circumstances, meet the definition of financial institution or creditor, and most certainly not a credit card issuer, they are obliged to comply with the third section of the rule that implements Section 315 of the FACT Act and applies to users of credit reports. Specifically, Section 315 requires users of consumer reports to develop reasonable policies and procedures that they must apply when they receive a notice of address discrepancy from a consumer reporting agency.

While apartment owners solely engaged in the business of renting apartments are not expressly obliged to comply with the rule in its entirety, given the complex nature of some business operations, firms are encouraged to familiarize themselves with the entire rule and to consult with counsel to ensure their overall compliance obligations.

The FTC is charged with enforcing the rule and can impose civil fines of up to $2,500 per violation for knowing violations of the rule that constitute a pattern or practice. They can also use their adjudication authority to issue cease and desist orders and take other enforcement actions. There is no private right of action for noncompliance. On October 22, 2008, the FTC announced that they will suspend enforcement of the new "Red Flags Rule" until May 1, 2009 to give creditors and financial institutions additional time in which to develop and implement written identity theft prevention programs. **This delay however does not extend to the rule regarding address discrepancies, which applies to apartment owners as users of consumer reports. Firms are still obliged to comply with that rule as of November 1, 2008.**

This memo answers frequently asked questions (FAQs) about the rule. The full rules are posted at http://edocket.access.gpo.gov/2007/pdf/07-5453.pdf.

Property owners are also reminded that the Red Flag and Address Discrepancy Rules are just two of the provisions included in the FACT Act of 2003 for which the federal agencies were required to issue regulations. The FACT Act amended the Fair Credit Reporting Act (FCRA) to impose strict new rules primarily on financial institutions and credit card companies and to grant consumers new protections against identity theft. The apartment industry as "users" and "furnishers" of credit report files, have more limited compliance obligations, but they are still extremely important.

The following is a list of compliance provisions apartment firms should include in their screening process and ID theft programs.

- **Data Destruction.** The FTC's Data Disposal Requirements require firms that use consumer reports, or information derived from such reports, to take "reasonable measures" to protect against unauthorized access to such data during disposal. This includes credit reports or scores, employment background checks, residential records or medical history. According to the rule, "reasonable measures" are flexible and could include burning, pulverizing or shredding papers that include consumer information. They also require firms to destroy or erase electronic media (e.g., e-mail, computer files) with such information so it cannot be read or reconstructed. (Additional information is available at www.nmhc.org/goto/3515.)

- **Adverse Action Notice.** When firms take an adverse action based solely or partly on the basis of the information derived from a consumer credit report, they must provide a notice of this action to the consumer. An adverse action can include denial of application for occupancy or requiring a co-signer on the lease.

- **Law Enforcement Requests.** Firms must comply with requests from law enforcement officials to turn over any records related to a transaction that may involve identity theft such as rental applications.

- **Debt Collection Prohibition.** Property owners and managers are prohibited from pursuing debt collection efforts with a third party if notice had been provided to the owner that the debt is the result of identity theft.

- **Refurnishing Information Prohibition.** Once property owners are notified by a consumer reporting agency (CRA) that consumer information provided by the owner is the result of identity theft, owners are prohibited from refurnishing that information to anyone else.

- **Reinvestigation of Consumer Information.** Under certain conditions, property owners will be required to reinvestigate the accuracy of information provided to a CRA if it is disputed by the consumer as being the result of identity fraud.

ADDITIONAL RESOURCES

- NMHC's FCRA/FACT Act Resource Center at www.nmhc.org/goto/FCRA
- FTC's FCRA Web Site at www.ftc.gov/privacy/privacyinitiatives/credit.html

FREQUENTLY ASKED QUESTIONS (FAQs) ABOUT THE FACT ACT'S RED FLAG AND ADDRESS DISCREPANCY RULES

SECTION 315: ADDRESS DISCREPANCY

Under rules in place since December 1, 2004, credit bureaus must notify the creditor, landlord, employer or other requester of a consumer report if the address supplied by the consumer "substantially differs" from the address included in the bureau's files.

Section 315 of the FACT Act requires credit report users (i.e., apartment firms) who receive an address discrepancy notice from a credit bureau to take additional steps to verify the identity of the person applying to open an account or rent a property.

1. **What is required under the Address Discrepancy Provision?**
   - The consumer reporting agency (CRA) must notify the end user (i.e., apartment professional) when there is an address discrepancy in a requested consumer file;
   - The end user, or apartment professional, must develop reasonable policies and procedures to determine the identity of the applicant when such notice of address discrepancy is received by the CRA; and
   - The end user must develop reasonable policies and procedures for furnishing the CRA with the accurate address of the consumer, under certain circumstances (see below).

2. **Who must comply?**
   The Rule states: "the Section 315 requirements apply to State-chartered credit unions, non-bank lenders, insurers, **landlords**, employers, mortgage brokers, automobile dealers, collection agencies, and any other person who requests a consumer report from a consumer reporting agency described in section 603(p) of the FCRA."

3. **What would be considered reasonable policies and procedures for determining the true identity of the consumer?**
   Reasonable policies would include comparing the consumer report information with:
   - information maintained in company's own records (i.e., previous residency files);
   - information obtained from third-party sources (i.e., resident screening companies or previous owners); and
   - information the end user gains from other regulatory requirements, such as Customer Identification Program (CIP) documentation required of financial institutions under the U.S. Patriot Act.

4. **When does an end user or apartment firm have to furnish the consumer's address to the CRA?**
   After receiving notification from a CRA of an address discrepancy, and upon reasonably confirming the accurate address for the consumer, the user/apartment provider must furnish this information to the CRA. if the following conditions are met:
   - the relationship with the consumer is a new one; and
   - the user regularly furnishes information to the CRA.

   This information should be furnished to the CRA as part of the information firms regularly furnish for the reporting period in which it establishes a relationship with the consumer.

5. **Must apartment owners maintain written policies and procedures for address discrepancies?**
   Unlike the Red Flags Rule (which follows), there is no express requirement that the required policies and procedures on address discrepancies be in writing. However, to ensure appropriate measures are being followed by employees company-wide, and to reduce the potential for violation, a written policy is highly recommended.

SECTION 114: RED FLAGS

1. What is a Red Flag?

A red flag is a pattern, practice or specific forms of activity, that indicates a possible existence of identify theft. An example of a red flag in the apartment context might be a fraud alert or credit freeze included with a consumer report. Another may be that photo identification provided appears to have been altered or forged. A list of 26 common red flags identified by the agencies follows this FAQ.

2. Are apartment owners/managers obliged to comply with the Red Flag rules?

Unlike Section 315, which specifically includes "landlord" as a covered entity, there is no similar language in Section 114, either in the FACT Act or the regulations implementing it. Therefore, a reasonable interpretation would suggest that rental property owners are not considered a financial institution or a creditor and therefore not required to meet the compliance obligations of this section. However, if your company operates, or is affiliated with, other businesses that may be interpreted as creditors, you may trigger such compliance. It is advised that you consult legal counsel about individual business obligations.

Having said that, while apartment owners may not technically be required to have an identity theft program in place, it is highly recommended that practices are in place to address red flags associated with potential ID theft as identified in this rule. Any policy and procedure firms establish to comply with the FACT Act's address discrepancy requirements can be expanded to address the broader red flag requirements with little added expense and time.

3. What is the general requirement of Section 114?

Section 114 of the Act requires financial institutions and creditors to establish a written identity theft prevention program to "detect, prevent and mitigate identity theft in connection with the opening of certain accounts or existing accounts." Interagency Guidelines were created to assist business entities with the development of a program and are attached as Appendix A. The Guidelines cover key elements of an Identity Theft Program, including: (1) Identifying Red Flags; (2) Detecting Red Flags; and (3) Responding to Red Flags.

4. Who Must comply with the Red Flags Rule?

Financial institutions and creditors with covered accounts must comply. The rule defines these entities as follows:

- *Financial Institution*: a state or national bank, a state or federal savings and loan association, a mutual savings bank, a state or federal credit union, or any other entity that holds a "transaction account" belonging to a consumer.
- *Transaction Account:* a deposit or other account from which the owner makes payments or transfers. Includes checking accounts, savings deposits subject to automatic transfers, and share draft accounts.
- *Creditor:* has the same meaning as in 15 U.S.C. 1681a(r)(5), and includes lenders such as banks, finance companies, automobile dealers, mortgage brokers, utility companies, and telecommunications companies.
- *Covered Account:* an account that a financial institution or creditor offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, such as a credit card account, mortgage loan, automobile loan, margin account, cell phone account, utility account, checking account, or savings account. A covered account is also an account for which there is a foreseeable risk of identity theft.

Common Red Flags for Identity Theft

Alerts, Notifications or Warnings from a Consumer Reporting Agency

1. A fraud or active duty alert is included with a consumer report.
2. A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.
3. A consumer reporting agency provides a notice of address discrepancy, as defined in § 681.1(b) of this part.
4. A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or customer, such as:
   - *A recent and significant increase in the volume of inquiries;*
   - *An unusual number of recently established credit relationships;*
   - *A material change in the use of credit, especially with respect to recently established credit relationships; or*
   - *An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.*

Suspicious Documents

5. Documents provided for identification appear to have been altered or forged.
6. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.
7. Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.
8. Other information on the identification is not consistent with readily accessible information that is on file with the financial institution or creditor, such as a signature card or a recent check.
9. An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

Suspicious Personal Identifying Information

10. Personal identifying information provided is inconsistent when compared against external information sources used by the financial institution or creditor. For example:
    - the address does not match any address in the consumer report; or
    - the Social Security number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File.
11. Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer. For example, there is a lack of correlation between the SSN range and date of birth.
12. Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example:
    - the address on an application is the same as the address provided on a fraudulent application; or
    - the phone number on an application is the same as the number provided on a fraudulent application.
13. Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example:
    - the address on an application is fictitious, a mail drop, or a prison; or
    - the phone number is invalid, or is associated with a pager or answering service.
14. The SSN provided is the same as that submitted by other persons opening an account or other customers.

15. The address or telephone number provided is the same as or similar to the account number or telephone number submitted by an unusually large number of other persons opening accounts or other customers.
16. The person opening the covered account or the customer fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.
17. Personal identifying information provided is not consistent with personal identifying information that is on file with the financial institution or creditor.
18. For financial institutions and creditors that use challenge questions, the person opening the covered account or the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

Unusual Use of, or Suspicious Activity Related to, the Covered Account

19. Shortly following the notice of a change of address for a covered account, the institution or creditor receives a request for a new, additional, or replacement card or a cell phone, or for the addition of authorized users on the account.
20. A new revolving credit account is used in a manner commonly associated with known patterns of fraud patterns. For example:
    - the majority of available credit is used for cash advances or merchandise that is easily convertible to cash (e.g., electronics equipment or jewelry); or
    - the customer fails to make the first payment or makes an initial payment but no subsequent payments.
21. A covered account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example:
    - nonpayment when there is no history of late or missed payments;
    - a material increase in the use of available credit;
    - a material change in purchasing or spending patterns;
    - a material change in electronic fund transfer patterns in connection with a deposit account; or
    - a material change in telephone call patterns in connection with a cellular phone account.
22. A covered account that has been inactive for a reasonably lengthy period of time is used (taking into consideration the type of account, the expected pattern of usage and other relevant factors).
23. Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account.
24. The financial institution or creditor is notified that the customer is not receiving paper account statements.
25. The financial institution or creditor is notified of unauthorized charges or transactions in connection with a customer's covered account.

Notice from Customers, Victims of Identity Theft, Law Enforcement Authorities, or Other Persons Regarding Possible Identity Theft in Connection with Covered Accounts Held by the Financial Institution or Creditor

26. The financial institution or creditor is notified by a customer, a victim of identity theft, a law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft.

Source: Federal Trade Commission 16 CFR Part 681, Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003; Final Rule, **Supplement A to Appendix A**

Appendix A: Interagency Guidelines on Identity Theft Detection, Prevention and Mitigation

Section 681.2 of the rules requires each financial institution and creditor that offers or maintains one or more covered accounts, as defined in § 681.2(b)(3) of this part, to develop and provide for the continued administration of a written Program to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account. These guidelines are intended to assist financial institutions and creditors in the formulation and maintenance of a Program that satisfies the requirements of Section 681.2 of this part.

I. The Program

In designing its Program, a financial institution or creditor may incorporate, as appropriate, its existing policies, procedures, and other arrangements that control reasonably foreseeable risks to customers or to the safety and soundness of the financial institution or creditor from identity theft.

II. Identifying Relevant Red Flags

(a) *Risk Factors.* A financial institution or creditor should consider the following factors in identifying relevant Red Flags for covered accounts, as appropriate:
   (1) The types of covered accounts it offers or maintains;
   (2) The methods it provides to open its covered accounts;
   (3) The methods it provides to access its covered accounts; and
   (4) Its previous experiences with identity theft.

(b) *Sources of Red Flags.* Financial institutions and creditors should incorporate relevant Red Flags from sources such as:
   (1) The types of covered accounts it offers or maintains;
   (2) The methods it provides to open its covered accounts;
   (3) The methods it provides to access its covered accounts; and
   (4) Incidents of identity theft that the financial institution or creditor has experienced;
   (5) Methods of identity theft that the financial institution or creditor has identified that reflect changes in identity theft risks; and
   (6) Applicable supervisory guidance.

(c) *Categories of Red Flags.* The Program should include relevant Red Flags from the following categories, as appropriate. Examples of Red Flags from each of these categories are appended as Supplement A to this Appendix A.
   (1) Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services;
   (2) The presentation of suspicious documents;
   (3) The presentation of suspicious personal identifying information, such as a suspicious address change;
   (4) The unusual use of, or other suspicious activity related to, a covered account; and
   (5) Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by the financial institution or creditor.

III. Detecting Red Flags

The Program's policies and procedures should address the detection of Red Flags in connection with the opening of covered accounts and existing covered accounts, such as by:

(a) Obtaining identifying information about, and verifying the identity of, a person opening a covered account, for example, using the policies and procedures regarding identification and verification set forth in the Customer Identification Program rules implementing 31 U.S.C. 5318(l) (31 CFR 103.121); and

(b) Authenticating customers, monitoring transactions, and verifying the validity of change of address requests, in the case of existing covered accounts.

IV. Preventing and Mitigating Identity Theft

The Program's policies and procedures should provide for appropriate responses to the Red Flags the financial institution or creditor has detected that are commensurate with the degree of risk posed. In determining an appropriate response, a financial institution or creditor should consider aggravating factors that may heighten the risk of identity theft, such as a data security incident that results in unauthorized access to a customer's account records held by the financial institution, creditor, or third party, or notice that a customer has provided information related to a covered account held by the financial institution or creditor to someone fraudulently claiming to represent the financial institution or creditor or to a fraudulent web site. Appropriate responses may include the following:

(a) Monitoring a covered account for evidence of identity theft;
(b) Contacting the customer;
(c) Changing any passwords, security codes, or other security devices that permit access to a covered account;
(d) Reopening a covered account with a new account number;
(e) Not opening a new covered account;
(f) Closing an existing covered account;
(g) Not attempting to collect on a covered account or not selling a covered account to a debt collector;
(h) Notifying law enforcement; or
(i) Determining that no response is warranted under the particular circumstances.

V. Updating the Program

Financial institutions and creditors should update the Program (including the Red Flags determined to be relevant) periodically, to reflect changes in risks to customers or to the safety and soundness of the financial institution or creditor from identity theft, based on factors such as:

(a) The experiences of the financial institution or creditor with identity theft;
(b) Changes in methods of identity theft;
(c) Changes in methods to detect, prevent, and mitigate identity theft;
(d) Changes in the types of accounts the financial institution or creditor offers or maintains; and
(e) Changes in the business arrangements of the financial institution or creditor, including mergers, acquisitions, alliances, joint ventures, and service provider arrangements.

VI. Methods for Administering the Program

(a) *Oversight of Program.* Oversight by the board of directors, an appropriate committee of the board, or a designated employee at the level of senior management should include:
  (1) Assigning specific responsibility for the Program's implementation;
  (2) Reviewing reports prepared by staff regarding compliance by the financial institution or creditor with § 681.2 of this part; and
  (3) Approving material changes to the Program as necessary to address changing identity theft risks.

(b) *Reports.*
  (1) *In general.* Staff of the financial institution or creditor responsible for development, implementation, and administration of its Program should report to the board of directors, an appropriate committee of the board, or a designated employee at the level of senior management, at least annually, on compliance by the financial institution or creditor with § 681.2 of this part.
  (2) *Contents of report.* The report should address material matters related to the Program and evaluate issues such as: The effectiveness of the policies and procedures of the financial institution or creditor in addressing the risk of identity theft in connection with the opening of covered accounts and with respect to existing covered accounts; service provider arrangements; significant incidents involving identity theft and management's response; and recommendations for material changes to the Program.

(c) *Oversight of service provider arrangements.*
Whenever a financial institution or creditor engages a service provider to perform an activity in connection with one or more covered accounts, the financial institution or creditor should take steps to ensure that the activity of the service provider is conducted in accordance with reasonable policies

and procedures designed to detect, prevent, and mitigate the risk of identity theft. For example, a financial institution or creditor could require the service provider by contract to have policies and procedures to detect relevant Red Flags that may arise in the performance of the service provider's activities, and either report the Red Flags to the financial institution or creditor, or to take appropriate steps to prevent or mitigate identity theft.

VII. Other Applicable Legal Requirements

Financial institutions and creditors should be mindful of other related legal requirements that may be applicable, such as:

(a) For financial institutions and creditors that are subject to 31 U.S.C. 5318(g), filing a Suspicious Activity Report in accordance with applicable law and regulation;

(b) Implementing any requirements under 15 U.S.C. 1681c–1(h) regarding the circumstances under which credit may be extended when the financial institution or creditor detects a fraud or active duty alert;

(c) Implementing any requirements for furnishers of information to consumer reporting agencies under 15 U.S.C. 1681s–2, for example, to correct or update inaccurate or incomplete information, and to not report information that the furnisher has reasonable cause to believe is inaccurate; and

(d) Complying with the prohibitions in 15 U.S.C. 1681m on the sale, transfer, and placement for collection of certain debts resulting from identity theft.