

All users of credit information must work to protect the privacy of consumers. By executing a Credit Reporting Subscriber Agreement with LandAmerica Credit Services, Inc. ("LACR"), Subscriber: (1) acknowledges that Subscriber has received the following Notice To Users of Access Security Requirements (the "Security Notice"); (2) warrants and represents that Subscriber has read and understood the Security Notice; (4) agrees that the Security Notice is an integral part of the Credit Reporting Subscriber Agreement and is binding on Subscriber; (5) acknowledges that the Security Notice may be unilaterally changed from time to time by LACR by electronically posting an amendment or modification on LACR's website at www.landamcredit.com or on LACR's user network and such changes shall be deemed effective when posted; (6) agrees to follow the security measures set forth in the Security Notice, the Credit Reporting Subscriber Agreement, and any amendments thereto, including, without limitation, the Confidentiality, Security and Privacy Amendment.

Revised January 5, 2005

NOTICE TO USERS OF ACCESS SECURITY REQUIREMENTS

1. The account number and password issued to Subscriber must be carefully protected so that only key personnel know this sensitive information. Unauthorized persons must not ever be given or have the opportunity to obtain knowledge of Subscriber's password. Neither account number nor the password are to be posted in any manner within Subscriber's facility or otherwise be subject to public or quasi-public access.
2. System access software, whether developed by your company or purchased from a third party vendor, must have Subscriber's account number and password "hidden" or embedded and be known only by supervisory personnel. Each user of Subscriber's system access software should be assigned a unique logon password and be required to take steps to protect it.
3. Subscriber's account number and passwords must never be discussed by telephone with any unknown caller, even if the caller claims to be an employee of LACR, a credit repository or an enforcement agency. Similarly, Subscriber's account number and passwords must never be provided to an unknown person via email or other means.
4. The ability to obtain credit information should be restricted to key personnel who have been properly trained and who are familiar with the FCRA.
5. All terminal devices, direct access terminals, desktop and laptop computers or other equipment or hardware used to obtain credit information are to be placed in a secure location within Subscriber's facility. These devices should be physically secure so that unauthorized persons cannot access them.
6. After normal business hours, or at any time they are left unattended for a significant period of time, all devices or systems used to obtain credit information are to be turned off and locked or otherwise secured.
7. All hard copies and electronic files of consumer reports within Subscriber's facility must be secured so that unauthorized persons cannot easily access them.
8. All hard copies of consumer reports are to be shredded or destroyed when no longer needed.

9. At such time as they are no longer needed and applicable regulation(s) permit destruction, electronic files containing consumer are to be permanently erased or scrambled.
10. All employees are to be informed that Subscriber may access credit information only for the permissible purposes listed in Subscriber Agreement and that they may not access their own report or the report of a family member or friend if Subscriber does not have permissible purpose and otherwise fully complies with the FCRA.
11. To the extent not already embodied by the measures describer above or already employed by Subscriber, Subscriber is urged to carefully consider implementing other appropriate measures to protect the privacy of consumers such as access controls (passwords, etc.), access restrictions (physical measures like locks, alarms, etc.), encryption, dual control procedures, segregation of duties, employee background checks, monitoring systems (designed to detect attacks and security breaches), reporting procedures, disaster protection, employee training and regular testing of all security measures.
12. Subscriber agrees that LACR and/or its vendors may periodically perform a security audit of Subscriber's compliance with the security requirements and any other required security requirements. Subscriber shall promptly implement correction of any deficiencies discovered in any such security audit.

Record Retention: It is important that credit applications are kept for a reasonable period of time. This will help to facilitate the investigative process if a consumer claims that Subscriber inappropriately accessed their credit report. (Note: The Federal Equal Credit Opportunity Act states that a creditor must preserve all written or recorded information connected with an application for 36 months; other applicable laws may require different holding periods.)

“Under Section 621 (a) (2) (A) of the FCRA, any person that violates any of the provisions of the FCRA may be liable for a civil penalty of not more than \$2,500 per violation.”