Expertise Support Accuracy Efficiency

ACCESS SECURITY REQUIREMENTS FOR DAILY USERS

We must work together to protect the privacy and information of consumers.
The following information security measures are designed to reduce unauthorized access to consumer information.

SUBSCRIBER CODES AND USER IDS

- Create a separate, unique user ID for each user to enable individual authentication and accountability for access to the credit reporting agency infrastructure. Each user of the system access software must also have a unique logon password.
- Ensure that user IDs are not shared and that no Peer-to-Peer file sharing is enabled on those users' profiles.

PASSWORDS AND SCREENSAVERS

- Do not provide your credit reporting agency Subscriber Codes or passwords to anyone. No one from the credit reporting agency will ever contact you and request your Subscriber Code number or password.
- Keep user passwords Confidential.
- Develop strong passwords that are:
  - Not easily guessable (i.e. your name or company name, repeating numbers and letters or consecutive numbers and letters)
  - Contain a minimum of seven (7) alpha/numeric characters for standard user accounts
  - Implement password protected screensavers with a maximum fifteen (15) minute timeout to protect unattended workstations.

CREDIT ACCESS AND LIMITATIONS

- Restrict the number of key personnel who have access to credit information.
- Ensure that personnel who are authorized to access credit information have a business need to access consumer credit information. Understand these requirements to access credit information are only for the permissible purpose listed in the Permissible Purpose Information section of your membership application.
- Ensure that you and your employees do not access your own credit reports or those reports of any family member(s) or friend(s) unless it is in connection with a credit transaction or for another permissible purpose.
- Implement a process to terminate access rights immediately for users who access credit reporting agency credit information when those users are terminated or when they have a change in their job tasks and no longer require access to that credit information.
- After normal business hours, turn off and lock all devices or systems used to obtain credit information
- Implement physical security controls to prevent unauthorized entry to your facility and access to systems used to obtain credit information
- Develop and follow procedures to ensure that data is protected throughout its entire information lifecycle (from creation, transformation, use, storage and secure destruction) regardless of the media used to store the data (i.e., tape, disk, paper, etc.)
- Only open email attachments and links from trusted sources and after verifying legitimacy.

MAINTAINING RECORDS

RECORD RETENTION: The Federal Equal Opportunities Act states that a creditor must preserve all written or recorded information connected with an application for 25 months. In keeping with the ECOA, the credit reporting agency requires that you retain the credit application and, if applicable, a purchase agreement for a period of not less than 25 months. When conducting an investigation, particularly following a breach or a consumer complaint that your company impermissibly accessed their credit report, the agency will contact you and will request a copy of the original application signed by the consumer or, if applicable, a copy of the sales contract.