

ACCESS SECURITY REQUIREMENTS
and
SECONDARY USE RESTRICTIONS AND REQUIREMENTS

It is a requirement that all Clients take precautions to secure any system or device used to access consumer reports, credit risk scores, and other sensitive information (collectively, "Information Services") from First Advantage CREDCO, LLC doing business as First American CREDCO and CredStar (collectively "FAC"). To that end, Client must comply with the following requirements:

1. Client's account number and password must be protected in such a way that this sensitive information is known only to Authorized Employees. Authorized Employees are employees of Client who have access to Information Services. Under no circumstances are unauthorized persons to have knowledge of your Client's password or account number. The information may not be posted in any manner within Client's facilities. Prior to providing an Authorized Employee with access to any Information Service, Client will provide the Authorized Employee with adequate training regarding these Access Security Requirements, the Fair Credit Reporting Act, the Gramm-Leach-Bliley Act, and other applicable laws, and will require the Authorized Employee to agree to comply with all such requirements and laws (together, "Employee Requirements"). Client will not add any employee as an Authorized Employee unless the employee has received the required training and has agreed to comply with the Employee Requirements. FAC will protect Client's access by enforcing a limit of 5 consecutive invalid access attempts by a user during a 30 minute period.
2. Any system access software Client uses, whether developed by Client or purchased from a third party vendor, must have Client's account number and password "hidden" or embedded so that the password is known only to Authorized Employees. Password files must be encrypted (128-bit encryption or stronger). Each Authorized Employee of Client's system access software must then be assigned unique log-ons and passwords.
3. User IDs and passwords must be deactivated immediately upon an Authorized Employee's termination or change of job assignment. User identifiers and logon processes may not be transmitted in clear-text across internal or external networks. All users are required to change passwords whenever there is any indication of possible system or password compromise. Passwords cannot be changed for a minimum of 10 days. The minimum password age must be set to 10 days on all systems. Passwords must not be the same for 5 consecutive times.
4. Password management must conform to the following best practices:
 - o Minimum 8 characters in length
 - o Mix of alpha, numeric, and special characters
 - o Passwords must expire every 90 days
 - o No re-use of a password for 6 months
 - o No automatic scripting of passwords
5. Client's account number and passwords are not to be discussed by telephone to any unknown caller, even if the caller claims to be an employee of FAC.
6. The ability to obtain Information Services must be restricted to Authorized Employees.
7. Any terminal devices used to obtain Information Services must be placed in a secure location within Client's facility. Access to the devices must be difficult for unauthorized persons.
8. Any devices/systems used to obtain Information Services must be turned off and locked after normal business hours, when unattended by Authorized Employees.
9. Hard copies and electronic files of Information Services are to be secured within Client's facility and protected against release or disclosure to unauthorized persons.
10. Hard copies of Information Services are to be shredded or destroyed, rendered unreadable, when no longer needed and when it is permitted to do so by applicable law.
11. Electronic files containing Information Services must be completely erased or rendered unreadable when no longer needed and when destruction is permitted by applicable law.
12. Software cannot be copied. Software is issued explicitly to Client solely to access Information Services.
13. Client employees will be forbidden to attempt to obtain Information Services on themselves, associates or any other persons, except in the exercise of their official duties.
14. Credit Reports will not be ordered for employment purposes unless approved in writing by FAC.

15. The only acceptable media for receiving and/or transmitting Information Services or any part thereof, are as follows:
 - o private networks;
 - o secure internet connections (if approved by FAC in writing);
 - o via traditional facsimile.
16. Information Services may not be received and/or transmitted through the following:
 - o via internet e-mail;
 - o via third party facsimile service providers.
17. Any person who knowingly and willfully obtains information on a consumer from a consumer reporting agency under false pretenses, shall be fined under title 18, United States Code, imprisoned for not more than 2 years, or both.
18. If unauthorized access to Information Services is discovered or suspected, Client shall immediately notify FAC and further undertake all remedial efforts within Client's power and control to cure such unauthorized access or use.
19. In the event Client intends to share with or otherwise disclose consumer reports or credit risk scores (together, "Credit Reports") to a third party (other than an Authorized Employee, the consumer to whom the report/scores relate, or as otherwise required by law), Client must (a) notify FAC's Compliance Department in writing prior to such sharing or disclosure, and (b) comply with FAC's Secondary Use policy which may be modified by FAC from time to time, a copy of which may be retrieved at <http://www.credco.com/legaldocuments/SecondaryUsePolicy.pdf>.
20. If employees of Client will be accessing Information Services via laptop computers, such laptop computers must have (a) full disc encryption (meaning, the hard drive is fully encrypted with at least AES 256-bit encryption), and (b) pre-boot authentication to encryption software (meaning, before the laptop's operating system starts, the employee must authenticate himself/herself, as applicable, with a password or token before the operating system will start).
21. Implement and follow current best security practices for computer virus detection scanning services and procedures:
 - Use, implement and maintain a current, commercially available computer virus detection/scanning product on all computers, systems and networks;
 - If you suspect an actual or potential virus, immediately cease accessing the system and do not resume the inquiry process until the virus has been eliminated;
 - On a weekly basis at a minimum, keep anti-virus software up-to-date by vigilantly checking or configuring auto updates and installing new virus definition files.
22. Implement and follow current best security practices for computer anti-Spyware scanning services and procedures:
 - Use, implement and maintain a current, commercially available computer anti-Spyware scanning product on all computers, systems and networks;
 - If you suspect actual or potential Spyware, immediately cease accessing the system and do not resume the inquiry process until the problem has been resolved and eliminated;
 - Run a secondary anti-Spyware scan upon completion of the first scan to ensure all Spyware has been removed from your computers;
 - Keep anti-Spyware software up-to-date by vigilantly checking or configuring auto updates and installing new anti-Spyware definition files weekly, at a minimum. If your company's computers have unfiltered or unblocked access to the Internet (which prevents access to some known problematic sites), then it is recommended that anti-Spyware scans be completed more frequently than weekly.
23. Only open email attachments and links from trusted sources and after verifying legitimacy.
24. Disable vendor FAC default passwords, SSIDs, and IP addresses on wireless access points and restrict authentication on the configuration of the access point.
25. Perform regular tests on information systems (port scanning, virus scanning, vulnerability scanning).