

EXHIBIT E

Access Security Requirements/Security Breach Notification

In accessing Avantus services, you agree to follow these security requirements:

1. Implement Strong Access Control Measures

- 1.1 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.
- 1.2 Proprietary or third party system access software must have credit reporting agency Subscriber Codes and password(s) hidden or embedded. Account numbers and passwords should be known only by supervisory personnel.
- 1.3 You must request your Subscriber Code password be changed immediately when:
 - (a) any system access software is replaced by system access software or is no longer used;
 - (b) the hardware on which the software resides is upgraded, changed or disposed of
- 1.4 Protect credit reporting agency Subscriber Code(s) and password(s) so that only key personnel know this sensitive information. Unauthorized personnel should not have knowledge of your Subscriber Code(s) and password(s).
- 1.5 Create a separate, unique user ID for each user to enable individual authentication and accountability for access to the credit reporting agency's infrastructure. Each user of the system access software must also have a unique logon password.
- 1.6 Ensure that user IDs are not shared and that no Peer-to-Peer file sharing is enabled on those users' profiles.
- 1.7 Keep user passwords Confidential.
- 1.8 Develop strong passwords that are:
 - (c) Not easily guessable (i.e. your name or company name, repeating numbers and letters or consecutive numbers and letters)
 - (d) Contain a minimum of seven (7) alpha/numeric characters for standard user accounts
- 1.9 Implement password protected screensavers with a maximum fifteen (15) minute timeout to protect unattended workstations.
- 1.10 Active logins to credit information systems must be configured with a thirty (30) minute inactive session, timeout.
- 1.11 Restrict the number of key personnel who have access to credit information.
- 1.12 Ensure that personnel who are authorized access to credit information have a business need to access such information and understand these requirements to access such information are only for the permissible purposes listed in the Permissible Purpose Information section of your membership application.
- 1.13 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.
- 1.14 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.
- 1.15 After normal business hours, turn off and lock all devices or systems used to obtain credit information.

- 1.16 Implement physical security controls to prevent unauthorized entry to your facility and access to systems used to obtain credit information.

2. Maintain a Vulnerability Management Program

- 1.1 Keep operating system(s), Firewalls, Routers, servers, personal computers (laptop and desktop) and all other systems current with appropriate system patches and updates.
- 1.2 Configure infrastructure such as Firewalls, Routers, personal computers, and similar components to industry best security practices, including disabling unnecessary services or features, removing or changing default passwords, IDs and sample files/programs, and enabling the most secure configuration features to avoid unnecessary risks.
- 1.3 Implement and follow current best security practices for Computer Virus detection scanning services and procedures:
 - (e) Use, implement and maintain a current, commercially available Computer Virus detection/scanning product on all computers, systems and networks.
 - (f) 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.
 - (g) 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.
- 1.4 Implement and follow current best security practices for computer anti-Spyware scanning services and procedures:
 - (h) Use, implement and maintain a current, commercially available computer anti-Spyware scanning product on all computers, systems and networks.

3. Access Security Requirements/Security Breach Notification

- (i) 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.
- (j) Run a secondary anti-Spyware scan upon completion of the first scan to ensure all Spyware has been removed from your computers.
- (k) 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.

4. Protect Data

- 4.1 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.)
- 4.2 All credit reporting agency data is classified as Confidential and must be secured to this requirement at a minimum.
- 4.3 Procedures for transmission, disclosure, storage, destruction and any other information modalities or media should address all aspects of the lifecycle of the information.
- 4.4 Encrypt all credit reporting agency data and information when stored on any laptop computer and in the database using AES or 3DES with 128-bit key encryption at a minimum.
- 4.5 Only open email attachments and links from trusted sources and after verifying legitimacy.

5. Maintain an Information Security Policy

- 5.1 Develop and follow a security plan to protect the Confidentiality and integrity of personal consumer information as required under the GLB Safeguard Rule.
- 5.2 Establish processes and procedures for responding to security violations, unusual or suspicious events and similar incidents to limit damage or unauthorized access to information assets and to permit identification and prosecution of violators.
- 5.3 The FACTA Disposal Rules requires that you implement appropriate measures to dispose of any sensitive information related to consumer credit reports and records that will protect against unauthorized access or use of that information.
- 5.4 Implement and maintain ongoing mandatory security training and awareness sessions for all staff to underscore the importance of security within your organization.

6. Build and Maintain a Secure Network

- 6.1 Protect Internet connections with dedicated, industry-recognized Firewalls that are configured and managed using industry best security practices.
- 6.2 Internal private Internet Protocol (IP) addresses must not be publicly accessible or natively routed to the Internet. Network address translation (NAT) technology should be used.
- 6.3 Administrative access to Firewalls and servers must be performed through a secure internal wired connection only.
- 6.4 Any stand alone computers that directly access the Internet must have a desktop Firewall deployed that is installed and configured to block unnecessary/unused ports, services and network traffic.
- 6.5 Encrypt Wireless access points with a minimum of WEP 128 bit encryption, WPA encryption where available.
- 6.6 Disable vendor default passwords, SSIDs and IP Addresses on Wireless access points and restrict authentication on the configuration of the access point.

7. Regularly Monitor and Test Networks

- 7.1 Perform regular tests on information systems (port scanning, virus scanning, vulnerability scanning).
- 7.2 Use current best practices to protect your telecommunications systems and any computer system or network device(s) you use to provide Services hereunder to access credit reporting agency systems and networks. These controls should be selected and implemented to reduce the risk of infiltration, hacking, access penetration or exposure to an unauthorized third party by:
 - (l) protecting against intrusions;
 - (m) securing the computer systems and network devices;
 - (n) and protecting against intrusions of operating systems or software.

“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.”

8. SECURITY BREACH NOTIFICATION

Customer shall notify Avantus of any breach of the security of consumer reporting data if the personal information of consumers was, or is reasonably believed to have been, acquired by an unauthorized person within 24 hours following discovery thereof.

In the event of such a breach, Customer agrees to cooperate with Avantus and its consumer reporting vendors in any investigation relating thereto. The nature and timing of any notifications required herein shall be under the control of Avantus's consumer reporting vendors, unless otherwise required by law.

For purposes of this Agreement, "breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

For purposes of this Agreement, "personal information" means an individual's first name or first initial and last name in combination with anyone or more of the following data elements, when either the name or the data elements are not encrypted:

- (1) Social security number.
- (2) Driver's license number.
- (3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

For purposes of this Agreement, "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

For purposes of this Agreement, "notice" may be provided by one of the following methods:

- (1) Written notice.
- (2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code.
- (3) E-mail notice when the Customer has an e-mail address for the subject persons.
- (4) Conspicuous posting of the notice on the web site of the Customer.

The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

The notification may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.

In the event the of a breach (1) Customer shall provide to each affected or potentially affected consumer, credit history monitoring services for a minimum of one year in which the consumer's credit history is monitored and the consumer receives daily notification of changes that may indicate fraud or ID theft from at least one of the national consumer credit reporting bureaus, and (2) Avantus's consumer reporting vendors and Avantus may assess End User an expense recovery fee.