Appendix B: User Access Security Policy 3.0 (Screening Solutions)

First Advantage

A Symphony Technology Group Company

User Access Security Policy 4.0

(First Advantage)

Published: September 16, 2005

Revised: January 1, 2010

By: First Advantage (FADV)

Proprietary and Confidential

Version	Revision	Date	Author	Reason / Description
1.0	Original	September 16, 2005	WorkPlace Solutions	Tailored to WPS Products
1.1	Revision	May 3, 2007	Asim Fareeduddin	Added mention of an end user to Section II
2.0	Revisions	February 1, 2008	Barbara Smith	Removed sentence in section I referencing echoed SPII. Changed “should” to “must” in reference to User IDs and/or password sharing in Section V. In section V. changed 15 minutes to 20 minutes in 9th paragraph.
3.0	Revised	April 15, 2009	Asim Fareeduddin Tracy Brady	Revised to reflect company name change.
4.0	Revised	January 1, 2010	Creighton Frommer	Revised to reflect company name change.

I. Objective of the Security Policy:

First Advantage (FADV) maintains and distributes information about consumers, some of which is considered "sensitive" nonpublic personal information. FADV has defined such information to be fully displayed Social Security Numbers ("SSN"), Drivers License Numbers ("DL"), and Dates of Birth ("DOB"). FADV developed and implemented this Security Policy in order to protect against the misuse of or unauthorized access to sensitive data by users of FADV's systems ("System"). This Policy documents the security requirements that must be followed by our Subscribers in order to gain and maintain access to sensitive data.

II. Access to this Security Policy:

This Policy has been developed for the sole use of the Subscriber and should not be duplicated or distributed to those that have not been assigned as an end user or the security administrator by the Subscriber.

III. Right to restrict access:

FADV may deny Subscriber access to all or part of the System without notice if Subscriber engages in any conduct or activities that FADV in its sole discretion believes violates any of the terms and conditions of the subscriber agreement or this Security Policy. If FADV denies Subscriber access to the System because of such a violation, the Subscriber shall have no right (1) to access through FADV any materials stored on the System or the Internet through FADV, (2) to obtain any credit(s) otherwise due to Subscriber, and such credit(s) will be forfeited, (3) to access third party services, merchandise or information on the System or the Internet through FADV, and FADV shall have no obligation to notify any third-party providers of services, merchandise or information nor any responsibility for any consequences resulting from lack of notification.

IV. Right to modify:

FADV reserves the right to update or modify this Security Policy at any time as may be necessary to further secure its System. Subscriber will be given reasonable advance notice of any such updates or modifications.

V. Policy Provisions

Subscribers must assign a security administrator(s) to take full responsibility for the requirements contained herein.

The security administrator is responsible for the ongoing administration of Subscriber's user identification codes ("User IDs"). This includes issuing a new User ID to a user and deactivating an active User ID for a user that no longer has a permissible purpose to access the System or that is no longer employed by the Subscriber. The Subscriber and security administrator agrees to keep such User IDs confidential and assign new User IDs only to those employees of the company who have a legitimate permissible purpose. Each individual user must have their own user ID and user IDs should not be shared.

The security administrator will be issued a special User ID that enables him/her to access the portions of the System used to manage User IDs or provided instructions on how to manage user IDs through FADV's account setup team. FADV will provide the administrator with training necessary to administer User IDs through the System. The security administrator, where possible, will need to establish the appropriate IP address ranges that are allowed for the user being added to the System.

Once a User ID (and default password) has been activated for a user, the user must change the default password on the first successful login attempt. Passwords and User IDs must be alphanumeric, 6 to 15 characters in length, must contain both letters and numbers, and passwords cannot be the same as the User ID. All passwords are stored in an encrypted state to prevent unauthorized access or viewing by the administrator. The security administrator agrees to audit said User IDs and passwords on a reasonable schedule to ensure adherence to this Policy.

FADV will require all users to reset their password when prompted by the system. Failure to reset passwords when prompted is a violation of this Security Policy and will result in the revocation of the User ID and the user's privilege to use the System.

FADV, on a reasonable schedule determined by FADV, will deactivate inactive User IDs. Once deactivated, the security administrator may be able to delete or reactivate the User ID as appropriate. If a deactivated user contacts FADV for reactivation, a security representative of FADV will contact the security administrator of the account as a follow up. The user may only be reactivated by the security administrator of the account. If the security administrator is not available, the User ID will remain deactivated until such time as it is reactivated by the account security administrator.

FADV reserves the right to monitor and/or conduct audits of Subscriber's User IDs and passwords.

User IDs and passwords and IP addresses may be changed or blocked from time to time by FADV to prevent unauthorized or suspicious access to services or misuse of its System. Where applicable, if the IP address submitted for a particular login does not match the IP address established by the security administrator for this User ID, the login will be denied. If routine monitoring reveals significant reason for an in-depth inquiry, FADV reserves the right to suspend the account and/or User ID, and/or conduct a full audit immediately without notification to the customer.

Subscriber agrees to take appropriate measures so as to protect against the misuse and/or unauthorized access of FADV data through any methods, including unauthorized access through or to Subscriber's User IDs or passwords. This includes implementing measures such as ensuring the appropriate use of screensavers (20 minute timeout maximum), not writing down passwords anywhere, not sharing User ID or password with anyone else, and promptly notifying the security administrator if the subscriber has any reason to believe their authentication credentials have been compromised. Such misuse or unauthorized access shall include any disclosure, release, viewing or other unauthorized access to social security numbers, driver's license numbers or dates of birth. Subscriber agrees that FADV may temporarily suspend Subscriber's access for up to ten (10) business days pending an investigation of Subscribers use or access. Subscriber agrees to cooperate fully with any and all investigations. If any misuse or unauthorized access is found, FADV may immediately terminate the agreement with Subscriber without notice or liability of any kind.

In the event that Subscriber learns or has reason to believe that sensitive FADV data has been disclosed or accessed by an unauthorized party, Subscriber will immediately give notice of such event to FADV. Furthermore, in the event that Subscriber has access to or acquires personally identifiable information (e.g., social security numbers, driver's license numbers or dates of birth) from FADV, the following shall apply: Subscriber acknowledges that upon unauthorized access to or misuse of such sensitive information (a "Security Event"), Subscriber shall, in compliance with law, notify the individuals whose information was disclosed that a Security Event has occurred. Also, Subscriber shall be responsible for any other legal obligations which may arise under applicable law in connection with such a Security Event.

VI. Redress

In the event that Subscriber's access has been suspended or Subscriber's agreement has been terminated under this policy, Subscriber may file a written request for review with FADV's Privacy, Security and Compliance Organization.