**Access Security Requirements**

The following information security controls are required to reduce unauthorized access to consumer information. It is Client's responsibility to implement these controls. Service Provider reserves the right to make changes to these Access Security Requirements without prior notification. The information provided herewith provides minimum baselines for information security.

In accessing Service Provider's web platform to view the Services, Client agrees to follow these security requirements. These requirements are applicable to all systems and devices used to access, transmit, process, or store Service Provider data received as part of the Services:

**1. Implement Strong Access Control Measures**

1.1 All Services credentials such as Account Number, account passwords, User names/identifiers (user IDs) and user passwords must be kept confidential and must not be disclosed to an unauthorized party. No one from Service Provider will ever contact you and request your credentials.

1.2 Intentionally deleted.

1.3 If the third party or third party software or proprietary system or software, used to access Service Provider data/systems, is replaced or no longer in use, the passwords should be changed immediately.

1.4 Create a unique user ID for each user to enable individual authentication and accountability for access to Service Provider's infrastructure. Each user of the system access software must also have a unique logon password.

1.5 User IDs and passwords shall only be assigned to authorized individuals based on least privilege necessary to perform job responsibilities.

1.6 User IDs and passwords must not be shared, posted, or otherwise divulged in any manner.

1.7 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 eight (8) alphabetic and numeric characters for standard user accounts

• For interactive sessions (i.e. non system-to-system) ensure that passwords/passwords are changed periodically (every 90 days is recommended)

1.8 Passwords (e.g. account passwords, user password) must be changed immediately when any suspicion of password being disclosed to an unauthorized party (see section 4.3 for reporting requirements)

1.9 Ensure that passwords are not transmitted, displayed or stored in clear text; protect all end user (e.g. internal and external) passwords using, for example, encryption or a cryptographic hashing algorithm also known as "one-way" encryption. When using encryption, ensure that strong encryption algorithm are utilized (e.g. AES 256 or above).

1.10 Implement password protected screensavers with a maximum fifteen (15) minute timeout to protect unattended workstations. Systems should be manually locked before being left unattended.

1.11 Active logins to credit information systems must be configured with a 30 minute inactive session timeout.

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 the Permissible Purpose Certification.

1.13 Client must NOT install Peer-to-Peer file sharing software on systems used to access, transmit or store Service Provider data.

1.14 Ensure that Client employees do not access their 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.

1.15 Implement a process to terminate access rights immediately for users who access Service Provider information when those users are terminated or when they have a change in their job tasks and no longer require access to that information.

1.16 Implement a process to perform periodic user account reviews to validate whether access is needed as well as the privileges assigned.

1.17 Implement a process to periodically review user activities and account usage, ensure the user activities are consistent with the individual job responsibility, business need, and in line with contractual obligations.

1.18 Implement physical security controls to prevent unauthorized entry to Client's facility and access to systems used to obtain credit information. Ensure that access is controlled with badge readers, other systems, or devices including authorized lock and key.

## 2. Maintain a Vulnerability Management Program

2.1 Keep operating system(s), firewalls, routers, servers, personal computers (laptops and desktops) and all other systems current with appropriate system patches and updates.

2.2 Configure infrastructure such as firewalls, routers, servers, tablets, smart phones, personal computers (laptops and desktops), and similar components to industry best security practices, including disabling unnecessary services or features, and removing or changing default passwords, IDs and sample files/programs, and enabling the most secure configuration features to avoid unnecessary risks.

2.3 Implement and follow current best security practices for computer virus detection scanning services and procedures:

• Use, implement and maintain a current, commercially available anti-virus software on all systems, if applicable anti-virus technology exists. Anti-virus software deployed must be capable to detect, remove, and protect against all known types malicious software such as viruses, worms, spyware, adware, Trojans, and root-kits.

• Ensure that all anti-virus software is current, actively running, and generating audit logs; ensure that anti-virus software is enabled for automatic updates and performs scans on a regular basis.

• If you suspect an actual or potential virus infecting a system, immediately cease accessing the system and do not resume the inquiry process until the virus has been eliminated.

## 3. Protect Data

3.1 Develop and follow procedures to ensure that Service Provider 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.).

3.2 Service Provider data is classified Confidential and must be secured to in accordance with the requirements mentioned in this document at a minimum.

3.3 Procedures for Service Provider data transmission, disclosure, storage, destruction and any other information modalities or media should address all aspects of the lifecycle of the information.

3.4 Encrypt all Service Provider data and information when stored electronically on any system including but not limited to laptops, tablets, personal computers, servers, databases using strong encryption such AES 256 or above.

3.5 Service Provider data must not be stored locally on smart tablets and smart phones such as iPads, iPhones, Android based devices, etc.

3.6 When using smart tablets or smart phones to access Service Provider data, ensure that such devices are protected via device pass-code.

3.7 Applications utilized to access Service Provider data via smart tablets or smart phones must protect data while in transmission such as SSL protection and/or use of VPN, etc.

3.8 Only open email attachments and links from trusted sources and after verifying legitimacy.

3.9 When no longer in use, ensure that hard-copy materials containing Service Provider data are crosscut shredded, incinerated, or pulped such that there is reasonable assurance the hard-copy materials cannot be reconstructed.

3.10 When no longer in use, electronic media containing Service Provider data is rendered unrecoverable via a secure wipe program in accordance with industry-accepted standards for secure deletion, or otherwise physically destroying the media (for example, degaussing).

## 4. Maintain an Information Security Policy

4.1 If applicable, develop and follow a security plan to protect the confidentiality and integrity of personal consumer information as required under the GLB Safeguards Rule.

4.2 Suitable to complexity and size of the organization, establish and publish information security and acceptable user policies identifying user responsibilities and addressing requirements in line with this document and applicable laws and regulations.

4.3 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. *If you believe Service Provider data may have been compromised, immediately notify Service Provider within twenty-four (24) hours or per agreed contractual notification timeline (See also Section 8).*

4.4 The FACTA Disposal Rules requires that Client 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.

4.5 Implement and maintain ongoing mandatory security training and awareness sessions for all staff to underscore the importance of security in the organization.

4.6 When using third party service providers (e.g. application service providers), other than Service Provider, to access, transmit, store or process data, ensure that service provider is compliant with Experian Independent Third Party Assessment (EI3PA) program, and registered in Experian list of compliant service providers. If the service provider is in process of becoming compliant, it is Client's responsibility to ensure the service provider is engaged with Experian and exception is granted in writing. *Approved certifications in lieu of EI3PA can be found in the Glossary section.*

## 5. Build and Maintain a Secure Network

5.1 Protect Internet connections with dedicated, industry-recognized firewalls that are configured and managed using industry best security practices.

5.2 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.

5.3 Administrative access to firewalls and servers must be performed through a secure internal wired connection only.

5.4 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.

5.5 Change vendor defaults including but not limited to passwords, encryption keys, SNMP strings, and any other vendor defaults.

5.6 For wireless networks connected to or used for accessing or transmission of Service Provider data, ensure that networks are configured and firmware on wireless devices updated to support strong encryption (for example, IEEE 802.11i) for authentication and transmission over wireless networks.

5.7 When using service providers other than Service Provider (e.g. software providers) to access Service Provider

systems, access to such other third party tools/services must require multi-factor authentication.

## 6. Regularly Monitor and Test Networks

6.1 Perform regular tests on information systems (port scanning, virus scanning, internal/external vulnerability scanning). Ensure that issues identified via testing are remediated according to the issue severity (e.g. fix critical issues immediately, high severity in 15 days, etc.)

6.2 Ensure that audit trails are enabled and active for systems and applications used to access, store, process, or transmit Service Provider data; establish a process for linking all access to such systems and applications. Ensure that security policies and procedures are in place to review security logs on daily or weekly basis and that follow-up to exceptions is required.

6.3 Use current best practices to protect telecommunications systems and any computer system or network device(s) used to provide Services hereunder to access Service Provider 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:

- protecting against intrusions;
- securing the computer systems and network devices;
- and protecting against intrusions of operating systems or software.

## 7. Mobile and Cloud Technology

To the extent Client is storing or accessing data through a cloud provider, or accessing Service Provider's applications or data from a mobile device. Client will ensure the following are in place:

7.1 Storing Service Provider data on mobile devices is prohibited. Any exceptions must be obtained from Service Provider in writing documented by a written amendment to the Agreement; additional security requirements will apply.

7.2 Mobile applications development must follow industry known secure software development standard practices such as OWASP and OWASP Mobile Security Project adhering to common controls and addressing top risks.

7.3 Mobile applications development processes must follow secure software assessment methodology which includes appropriate application security testing (for example: static, dynamic analysis, penetration testing) and ensuring vulnerabilities are remediated.

7.4 Mobility solution server/system should be hardened in accordance with industry and vendor best practices such as Center for Internet Security (CIS) benchmarks, NIS, NSA, DISA and/or other.

7.5 Mobile applications and data shall be hosted on devices through a secure container separate from any personal applications and data. See details below. Under no circumstances is Service Provider data to be exchanged between secured and non-secured applications on the mobile device.

7.6 In case of non-consumer access, that is, commercial/business-to-business (B2B) users accessing Service Provider data via mobile applications (internally developed or using a third party application), ensure that multi-factor authentication and/or adaptive/risk-based authentication mechanisms are utilized to authenticate users to application.

7.7 When using cloud providers, other than Service Provider, to access, transmit, store, or process Service Provider data ensure that:

- Appropriate due diligence is conducted to maintain compliance with applicable laws and regulations and contractual obligations
- Cloud providers must have gone through independent audits by Client and are compliant with one or more of the following standards, or a current equivalent as approved/recognized by Service Provider:
  - ISO 27001
  - PCI DSS
  - EI3PA

- SSAE 16 – SOC 2 or SOC3
- FISMA
- CAI / CCM assessment

**8. General**

To the extent Client uses a third party system or software, other than Service Provider's system, Client will ensure the following are in place:

**8.1** Service Provider may from time to time audit the security mechanisms Client maintains to safeguard access to Service Provider information, systems and electronic communications. Audits may include examination of systems security and associated administrative practices

**8.2** In cases where the Client is accessing Service Provider information and systems via third party software, the Client agrees to make available to Service Provider upon request, audit trail information and management reports generated by the vendor software, regarding Client individual Authorized Users.

**8.3** Client shall be responsible for and ensure that third party software, which accesses Service Provider information systems, is secure, and protects this vendor software against unauthorized modification, copy and placement on systems which have not been authorized for its use.

**8.4** Client shall conduct software development (for software which accesses Service Provider information systems; this applies to both in-house or outsourced software development) based on the following requirements:

**8.4.1** Software development must follow industry known secure software development standard practices such as OWASP adhering to common controls and addressing top risks.

**8.4.2** Software development processes must follow secure software assessment methodology which includes appropriate application security testing (for example: static, dynamic analysis, penetration testing) and ensuring vulnerabilities are remediated.

**8.4.3** Software solution server/system should be hardened in accordance with industry and vendor best practices such as Center for Internet Security (CIS) benchmarks, NIS, NSA, DISA and/or other.

**8.5** Reasonable access to audit trail reports of systems utilized to access Service Provider systems shall be made available to Service Provider upon request, for example during breach investigation or while performing audits

**8.6** Data requests from Client to Service Provider must include the IP address of the device from which the request originated (i.e., the requesting client's IP address), where applicable.

**8.7** Client shall report actual security violations or incidents that impact Service Provider to Service Provider within twenty-four (24) hours or per agreed contractual notification timeline. Client agrees to provide notice to Service Provider of any confirmed security breach that may involve data related to the contractual relationship, to the extent required under and in compliance with applicable law. Telephone notification is preferred at 800-888-5773, Email notification will be sent to privacy@fadv.com.

**8.8** Client acknowledges and agrees that the Client (a) has received a copy of these requirements, (b) has read and understands Client's obligations described in the requirements, (c) will communicate the contents of the applicable requirements contained herein, and any subsequent updates hereto, to all employees that shall have access to Service Provider services, systems or data, and (d) will abide by the provisions of these requirements when accessing Service Provider data.

**8.9** Client understands that its use of Service Provider networking and computing resources may be monitored and audited by Service Provider, without further notice.

**8.10** Client acknowledges and agrees that it is responsible for all activities of its employees/Authorized users, and for assuring that mechanisms to access Service Provider services or data are secure and in compliance with its membership agreement.

**8.11** When using third party service providers to access, transmit, or store Service Provider data, additional documentation may be required by Service Provider.

*Record Retention: If applicable, the Federal Equal Credit Opportunity Act states that a creditor must preserve all written or recorded information connected with an application for 25 months. In keeping with the ECOA, Service Provider 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 consumer complaint that your company impermissibly accessed their credit report, Service Provider 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.*
*"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 $3,500 per violation."*

**Internet Delivery Security Requirements**
In addition to the above, following requirements apply where Client and their employees or an authorized agent/s acting on behalf of the Client are provided access to Service Provider provided services via Internet ("Internet Access").

**General requirements:**
1. Client agrees to designate in writing, an employee to be its Head Security Designate, to act as the primary interface with Service Provider on systems access related matters. The Client's Head Security Designate will be responsible for establishing, administering and monitoring all Client employees' access to Service Provider provided services which are delivered over the Internet ("Internet access"), or approving and establishing Security Designates to perform such functions.

2. The Client's Head Security Designate or Security Designate shall in turn review all employee requests for Internet access approval. The Head Security Designate or its Security Designate shall determine the appropriate access to each Service Provider product based upon the legitimate business needs of each employee. Service Provider shall reserve the right to terminate any accounts it deems a security threat to its systems and/or consumer data.

3. An officer of the Client agrees to notify Service Provider in writing immediately if it wishes to change or delete any employee as a Head Security Designate, Security Designate, or Authorized User; or if the identified Head Security Designate, Security Designate or Authorized User is terminated or otherwise loses his or her status as an Authorized User.

**Designate**
1. Must be an employee and duly appointed representative of Client, identified as an approval point for Client's Authorized Users.

2. Is responsible for the initial and on-going authentication and validation of Client's Authorized Users and must maintain current information about each (phone number, valid email address, etc.).

3. Is responsible for ensuring that proper privileges and permissions have been granted in alignment with Authorized User's job responsibilities.

4. Is responsible for ensuring that Client's Authorized Users are authorized to access Service Provider products and services.

5. Must disable Authorized User ID if it becomes compromised or if the Authorized User's employment is terminated by Client.

6. Must immediately report any suspicious or questionable activity to Service Provider regarding access to Service Provider's products and services.

7. Shall immediately report changes in their Head Security Designate's status (e.g. transfer or termination) to Service Provider.

8. Will provide first level support for inquiries about passwords/passphrases or IDs requested by your Authorized Users.
9. Shall be available to interact with Service Provider when needed on any system or user related matters.

**Glossary**

| Term | Definition |
|---|---|
| **Computer Virus** | A Computer Virus is a self-replicating computer program that alters the way a computer operates, without the knowledge of the user. A true virus replicates and executes itself. While viruses can be destructive by destroying data, for example, some viruses are benign or merely annoying. |
| **Confidential** | Very sensitive information. Disclosure could adversely impact Client. |
| **Encryption** | Encryption is the process of obscuring information to make it unreadable without special knowledge. |
| **Firewall** | In computer science, a Firewall is a piece of hardware and/or software which functions in a networked environment to prevent unauthorized external access and some communications forbidden by the security policy, analogous to the function of Firewalls in building construction. The ultimate goal is to provide controlled connectivity between zones of differing trust levels through the enforcement of a security policy and connectivity model based on the least privilege principle. |
| **Information Lifecycle** | (Or Data Lifecycle) is a management program that considers the value of the information being stored over a period of time, the cost of its storage, its need for availability for use by authorized users, and the period of time for which it must be retained. |
| **IP Address** | A unique number that devices use in order to identify and communicate with each other on a computer network utilizing the Internet Protocol standard (IP). Any All participating network devices - including routers, computers, time-servers, printers, Internet fax machines, and some telephones - must have its own unique IP address. Just as each street address and phone number uniquely identifies a building or telephone, an IP address can uniquely identify a specific computer or other network device on a network. It is important to keep your IP address secure as hackers can gain control of your devices and possibly launch an attack on other devices. |
| **Peer-to-Peer** | A type of communication found in a system that uses layered protocols. Peer-to-Peer networking is the protocol often used for reproducing and distributing music without permission. |
| **Router** | A Router is a computer networking device that forwards data packets across a network via routing. A Router acts as a junction between two or more networks transferring data packets. |
| **Spyware** | Spyware refers to a broad category of malicious software designed to intercept or take partial control of a computer's operation without the consent of that machine's owner or user. In simpler terms, spyware is a type of program that watches what users do with their computer and then sends that information over the internet. |
| **Account Number** | Your Service Provider account number. |
| **Experian Independent Third Party Assessment Program** | The Experian Independent 3rd Party Assessment is an annual assessment of a service provider's ability to protect the information they purchase from Experian.<br>EI3PA℠ requires an evaluation of a service provider's information security by an independent assessor, based on requirements provided by Experian.<br>EI3PA℠ also establishes quarterly scans of networks for vulnerabilities. |
| **ISO 27001 /27002** | IS 27001 is the specification for an ISMS, an Information Security |

| | |
|---|---|
| | Management System (it replaced the old BS7799-2 standard)<br>The ISO 27002 standard is the rename of the ISO 17799 standard, and is a code of practice for information security. It basically outlines hundreds of potential controls and control mechanisms, which may be implemented, in theory, subject to the guidance provided within ISO 27001. |
| **PCI DSS** | The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and POS cards. |
| **SSAE 16 SOC 2, SOC3** | Statement on Standards for Attestation Engagements (SSAE) No. 1<br>SOC 2 Report on Controls Related to Security, Availability, Processing Integrity, Confidentiality, and Privacy.<br>The SOC 3 Report, just like SOC 2, is based upon the same controls as SOC 2, the difference being that a SOC 3 Report does not detail the testing performed (it is meant to be used as marketing material). |
| **FISMA** | The Federal Information Security Management Act (FISMA) is United States legislation that defines a comprehensive framework to protect government information, operations and assets against natural or man-made threats. FISMA was signed into law part of the Electronic Government Act of 2002. |
| **CAI / CCM** | Cloud Security Alliance Consensus Assessments Initiative (CAI) was launched to perform research, create tools and create industry partnerships to enable cloud computing assessments.<br>The Cloud Security Alliance Cloud Controls Matrix (CCM) is specifically designed to provide fundamental security principles to guide cloud vendors and to assist prospective cloud customers in assessing the overall security risk of a cloud provider. |