

A Matter of Fact Client Access Security Requirements

Revised 2/12/2011

A Matter of Fact fully recognizes its obligation to support and implement policies that protect the confidential nature of the information we handle and assure respect for consumers' rights to privacy. Only companies who are approved clients and have a permissible purpose for obtaining credit information are permitted access to credit products.

It is a requirement that all A Matter of Fact clients take precautions to secure any system or device used to access consumer information. To that end, the following requirements have been established:

- Usernames and passwords must be protected in such a way that usernames and passwords are known only to authorized persons. Under no circumstances should unauthorized persons have knowledge of your password. The information should not be posted in any manner within your work area or facility.
- Any system access software you may use, whether developed by your company or purchased from a third party vendor, must have your password "hidden" or embedded so that the password is known only to supervisory personnel. Each user of your system access software must then be assigned unique logon passwords.
- Your A Matter of Fact username and password are not to be released to anyone, even someone who claims to be an A Matter of Fact employee. A Matter of Fact will never ask you for your password.
- The ability to obtain credit information from A Matter of Fact must be restricted to a few key personnel.
- Access to consumer information is restricted to authorized persons and authorized persons alone. Authorization to obtain or process Consumer information, or to access any system or device used to obtain or process Consumer information, is restricted to those employees with a legal permissible purpose to do so.
- Any terminal device used to obtain consumer or credit information should be placed in a secure location within your work site or facility. Access to the device should be difficult for unauthorized persons.
- Any devices/systems used to obtain or process consumer information should be turned off and locked after normal business hours or when unattended by authorized persons.
- Access to any devices/systems used to obtain or process consumer information should be protected by a username, a strong password, and by a hardware firewall. Such devices should not be accessible via local wireless connections. Under no circumstances should unauthorized persons have access to consumer information.
- Confidential consumer data is to be transmitted over the Internet **ONLY** via encrypted links (e.g. SSL or VPN) or by sending encrypted files. **NOTE:** If using a Fax to Email service or an Email to Fax service, please verify that all consumer information is securely stored and transmitted within your supplier's systems and between you and your supplier.
- **FULL SOCIAL SECURITY NUMBERS** are **NEVER** to be transmitted via Email. **NOTE:** If using a Fax to Email service or an Email to Fax service, please verify that all consumer information is securely stored and transmitted within your supplier's systems and between you and your supplier.
- Hard copy consumer reports are to be secured within your work site and protected against release or disclosure to unauthorized persons.
- Any consumer information stored on portable and/or removable electronic devices shall be encrypted.
- Following FTC Guidelines, work papers, consumer information and consumer reports are to be shredded/destroyed and/or deleted from any system or device when they are no longer needed and as soon as it is permitted to do so by applicable regulation(s) and law (including the Fair Credit Reporting Act and the Drivers Privacy Protection Act), taking measures to reasonably ensure that all such records and data are destroyed and unrecoverable.
- When no longer in use media (hard drives, floppy disks, DVDs, etc.) that have contained consumer information must be shredded/destroyed, according to applicable regulations, including the Fair Credit Reporting Act and the Drivers Privacy Protection Act.
- Procedures are in place to reasonably detect, investigate and respond to an information system intrusion, including consumer and/or customer notification where warranted.

By signing below you agree to comply with the above requirements. Please return signed copy by fax to 530-346-6620.

Company Name

First Name Last Name

Date