

Information Security Policy, Privacy Policy and Access Security Requirements

A Matter of Fact fully recognizes its obligation to support and implement policies that protect the confidential nature of the information we handle and to ensure respect for consumers' rights to privacy.

Client Obligations

Only companies who are approved clients and have a permissible purpose for obtaining information are permitted access to our products.

Clients are Required to Sign Agreements That Certify Each of the Following:

- All information and reports will be requested and used in accordance with the FCRA -- Fair Credit Reporting Act (including disclosure, written authorization, and copy distribution requirements).
- Information and reports will not be used in violation of any federal or state equal opportunity law or regulation.
- All information and reports obtained from A Matter of Fact will be requested and used in accordance with all applicable local, state, and federal laws and regulations (including disclosure, written authorization, and copy distribution requirements).
- The information requested will only be used for employment purposes and only for the client's own use.

Clients Agree to These Access Requirements:

- 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 authorized personnel.
- 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.

A Client Certification Is Required For Each Order:

A Matter of Fact requires that the following certification be made each time a background check is requested: "I certify that this request is made in accordance with FCRA (Fair Credit Reporting Act), Americans with Disabilities Act, and all other applicable local, state, and federal laws and regulations, including written disclosure to the consumer that a background check will be conducted, written authorization from the consumer to conduct the background check, receipt by the consumer of a copy of the report as required by law, and notification to the consumer including the name, address, and phone of the consumer reporting agency conducting the background check and a summary of the consumer's rights. I certify that 1) all required steps have been taken, and 2) all required steps will be taken. I also certify that the information requested will be used only for employment purposes and only for the employer's own use."

Employee, Subcontractor, and Vendor Obligations

A Matter of Fact requires that all employees, subcontractors, and vendors hold Consumer information in strictest confidence, and requires them to take the following precautions to secure any system, device, or data used in the obtaining or processing of Consumer information:

- 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 authorized personnel.
- 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.

Website Privacy

A Matter of Fact maintains several websites for the purpose of providing information to the public. Please see the privacy statement provided on each website.

Notices

This policy has been developed in accordance with local, state and federal law and the National Association of Professional Background Screeners (NAPBS) Provider Data Security Privacy Guidelines. The Operations Manager is responsible for implementing, managing and enforcing this policy.

Locked Facility

A Matter of Fact is a locked facility. All visitors are met at the door by an authorized employee of A Matter of Fact and are not left unattended while in our offices. Visitors are not given access to consumer information unless legally authorized in writing.

Consumer Files

A Matter of Fact is not an investigative consumer reporting agency that compiles and maintains files on consumers on a nationwide basis. The only files maintained by A Matter of Fact are archived copies of background check files as required by law. No information from a prior background check is used in a subsequent background check. Each report is compiled separately from fresh research data.

Consumer Requests for Information about their Background Checks

Proper identification is required before A Matter of Fact personnel will discuss or provide copies of a Consumer Report to a requesting consumer.

Personal Information Disclosure: United States or Overseas

A Matter of Fact subscribes to the standards of ConcernedCRAs regarding the off-shoring of sensitive personal information. See concernedcras.com/no_offshoring.htm. A Matter of Fact does not transfer consumer personally identifiable information to third-parties outside of the USA or its territories except through authorized access as required to conduct international record checks.

Personally Identifiable Information That May Be Collected About Individual Consumers

- first, middle, and last names
- home or other physical addresses, including street names and names of a city or town
- e-mail addresses
- telephone numbers
- social security numbers
- other identifiers that permit the physical or online identification of a specific individual

Third-Party Persons Or Entities With Whom A Matter Of Fact May Share Personally Identifiable Information

A Matter of Fact may contact individuals, corporations and other private/public entities or any of their employees or agents to check employment histories, references, educational achievements, licenses, certifications, credit reports, social security number scans, address histories, criminal records, civil court filings, driving records, workers comp records, or for any other research in connection with the processing of employment background checks.

Privacy Policy Update Notification

A Matter of Fact publishes privacy policy changes on the website www.amof.info.

Privacy Contact

The following can be contacted for assistance with additional information regarding A Matter of Fact's privacy practices or policies.

Customer Service
P.O. Box 1113
Colfax, CA 95713
530-346-6626
information@amof.info

Effective Date: 9/2/2011