Consumer Protection

Information Security Policy

- Information Security Policy (This is also provided as a separate document)

S2Verify Compliance with this Clause

S2Verify has developed and maintains policies and procedures to insure information security over five broad areas within our environment:

- Confidentiality
- Physical Security
- Electronic Security
- Communication Security
- Portable Electronic Storage Devices

The following is an overview of our information security principles and areas of emphasis. Each of the following broad areas has multiple, detailed procedures for insuring the information security.

Information Policy Fundamentals:

- Confidentiality

Access to confidential consumer information is limited to those who have a legitimate need to know the information. Those with a legitimate need to have consumer information are Vendors, Clients, Employees and Consumers. In addition, information is truncated unless on all reports and request unless it is absolutely necessary for the Vendor, Client or Employee.

Vendors, Clients and Employees are vetted, only provided/granted access/information necessary to their legitimate needs and then contractually bound to keep all information confidential. Consumers are vetted before information is disclosed.

Employees are prohibited from "browsing" files or databases without a business justification and the prohibition is contractually bound.

We maintain records on each request for information and identify each user who requested information on a consumer.

Destruction of consumer information follows the Federal Trade Commission's requirements that the information be unreadable upon disposal.

- Physical Security

Access to our computer terminals, file cabinets, fax machines, trash bins, desktops, etc. are secure from unauthorized access. Our offices are securely locked and monitored by an alarm system. Key Fab entry is required for all employees. Authorized visitors to our facility are checked in and monitored at all times while in the facility.

- Electronic Security

We maintain a secure network to safeguard consumer information from internal and external threat. Our backup data is maintained in an encrypted form. Access by users over the internet requires a confidential user name and strong password.

- Communication Security

All Consumer Information transmitted using our computer network, including email, is secured using a minimum of 128-bit SSL encryption. No Consumer Information is sent over the internet that is not encrypted or secured with a minimum of 128-bit SSL encryption or all SPII are truncated. This includes the body of emails and/or attachments. Access by users over the internet requires a confidential user name and strong password. Other means of communication i.e., fax and mail have specialized procedures to insure communication security including all SPII is truncated on all documentation.

- Portable Electronic Storage Devices

Consumer Protection

The storage of any consumer information outside the premises on any portable electronic storage device or media is prohibited and contractually agreed to by employees with the exception of secure transport of backup materials to an approved, vetted storage facility.

(See Appendix A, All Sections Policy and Procedure Manual for Employee Information Security)

(See Appendix B, All Sections for Deverus Technology for Full Data Security Technology Policy)

(See Appendix L All Sections for Information Security Policy)

Consumer Protection

Data Security Model

- Data Security Policy and Procedures Language

S2Verify Compliance with this Clause

Protecting consumer information from internal and external unauthorized access is of critical importance to S2Verify. Our policies and procedures address a wide range of areas to protect unauthorized access from both internal and external threats. Specifically, these include, but are not limited to:

Securing unattended workstations

Our policy is to require employees who are working with consumer information to log out of the system if they leave their workstation. Paper files, containing consumer information must also be secured if leaving their work area.

Limited access to networks, data, and work areas

Access to confidential consumer information is limited to those who have a legitimate need to know the information. Those with a legitimate need to have consumer information are Vendors, Clients, Employees and Consumers.

Vendors, Clients and Employees are vetted, only provided/granted access/information necessary to their legitimate needs and then contractually bound to keep all information confidential. Consumers are vetted before information is disclosed.

Work areas S2Verify Personnel

Employees are issued Key Fab and/or access pass-codes only to areas in which they are authorized by management to perform their job. The supervisor of the individual will authorize needed keys and/or access codes upon hire or a change in job assignment.

S2Verify Visitors/Guests/Vendors

While on the premises, visitors are escorted at all times and will not have access to SPII on computer screens, hard copy or electronic media of any type.

S2Verify Temporary/Contract Workers

Temporary or contract workers are, as rule, not granted access to areas that contain consumer information that is not locked in a secure location. If a temporary or contract worker is considered for a position requiring access to a secure area, they must first undergo the due diligence and make the same certifications as an employee would.

Limiting consumer information provided to information sources to only that information which is needed to conduct a search,

As described in Policy and Procedure 1.12, S2Verify policy is to truncate the SSN in any form outside our company unless the information is required by the client/vendor, allowed by law and securely transported. Specifically, SSNs are truncated to any entity outside our firm unless:

1. The full SSN is required to perform the search requested (e.g., employment verification) **or**
2. The full SSN is demanded to be returned by the client **and**,

    a. The disclosure is not prohibited by law **and**
    b. The data is limited to that which is needed **and**
    c. Secure transport methods (Policy and Procedures 1.2 and 4.5) are used.
3. The full SSN is never sent via US standard mail. All SPII is truncated on all documents that are sent to clients or consumers.

Our policy regarding other sensitive data is similar. Specifically,

4. We do not send out a full name with either the DOB or driver license number unless it is required by the client/vendor and securely transported (Policy and Procedure 4.5).

Our procedure is to set up each client and vendor template to not send the SSN/Name and DOB or DL number unless approved by appropriate supervisory permission.

Destruction of hard copy documents

S2Verify policy is to destroy/render inaccessible/unreadable and or unrecoverable all consumer and client information per current FTC rules.

Our procedure for destruction of hard copy documents is detailed in Policy and Procedure 1.10, Record Destruction.

Identification of caller before providing consumer information,

As detailed in Policy and Procedure 6.5, S2Verify requires that all consumers be identified and authenticated prior to disclosure of consumer information.

Our procedure is to obtain the consumer's full name, date of birth and last four digits of the SSN. A full name and driver's license number will also suffice as an alternative. Regardless of method used, we retain a written record of the information used to identity/authenticate the consumer.

Employee identification system

S2Verify is currently of the size where every employee is immediately identifiable to every other employee and new hires/terminations are known.

If an employee should see an unidentified individual in the premises, they should immediately address the individual to ascertain the individual's status/permission.

Unescorted visitor policy

As detailed in Policy and Procedure 6.9, S2Verify has implemented a visitor security policy to insure visitors do not access consumer information.

All visitors moving beyond our reception area must sign a registry upon arrival and are checked out upon departure. The registry contains the date, person they wish to see, reason for visit and time of arrival/departure.

While on the premises, visitors shall be escorted at any time when consumer information is available on computer screens, hard copy or electronic media of any type.

Secure transport of information

Physical transport of consumer information is done for data backup purposes. Our policy is to secure this information while in transit and our procedures are detailed in Policy and Procedure 1.4, Stored Data Security.

Use of encryption and/or secure networks and/or websites

All Consumer Information transmitted using our computer network, secured using a minimum of 128-bit SSL encryption. No Consumer Information is sent over the internet that is not encrypted or secured with a minimum of 128-bit SSL encryption. This includes the body of emails or attachments. Access by users over the internet requires a confidential user name and strong password. If any consumer information is sent via email and not encrypted, all SPII is truncated.

Password assignment and replacement

S2Verify policy is to issue unique usernames to each employee for each system the employee is authorized to access, to require the use of a strong password (a minimum of six (6) characters), and to require that each password be changed at least once every 120 days. Employees agree to treat passwords as confidential information and are prohibited from writing them down or sharing them with any other individual, inside or outside of the company. Our employee who is responsible for password protocol securely maintains records of issuance.

Our procedure is to periodically review this policy with each employee and confirm their understanding. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Controlling use of portable storage devices

The storage of any consumer information outside the premises on any portable electronic storage device or media is prohibited and contractually agreed to by employees with the exception of secure transport of backup materials to an approved, vetted storage facility.

Alarm systems

S2Verify premises are secured by a monitored alarm system. The system is on 24/7 and only authorized personnel with a key fab have access.

Door locks

Doors to all secure areas are locked at all times, during and after business hours. Only authorized personnel have keys and/or access codes to their authorized areas. Employees are issued key fab and/or key and they only have access to areas in which they are authorized by management to perform their job. The supervisor of the individual will authorize needed keys and/or access codes upon hire or a change in job assignment.

Secure server and back-up sites

S2Verify's policy is to ensure backup data is encrypted, and stored in a locked location.

Our procedure is to entrust all backups to our software platform vendor. We do not backup locally.

Our software platform vendor has certified that all of our backup data is encrypted and stored in a secure facility. See attached certification letter.

(See Appendix A, Section 1, 1.2 Policy and Procedure Manual for full Data Security Policy-Personnel)

(See Appendix B, Deverus Technology for full Data Security Policy Technology)

Consumer Protection

Intrusion, Detection and Response Model

• Intrusion, Detection and Response Policy and Procedure

S2Verify uses various tools, policies and procedures to protect against unauthorized access to our computer systems and consumer data. Specifically, we:

- Locate computers and servers that store consumer information in an access controlled environment;
- Utilize firewalls to protect all computers and servers, including those storing consumer information;
- Utilize commercial grade anti-virus and intrusion detection software on all computers and servers;
- Disallow connection of analog telephone lines to any computer or server that stores consumer information;
- Isolate any computer or server that communicates via File Transfer Protocol (FTP).
- Encrypt any data removed off-site for backups
- Require all employees to immediately notify their supervisor of any actual or suspected security breach involving files containing consumer information.

We require that only authorized personnel are permitted to implement and maintain the above mentioned technology. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

If an information system intrusion does occur, our procedure is to:

- Immediately inform the Information Technology Manager and President of the company. If the IT manager and President are unavailable, our supervisor of operations should be notified.
- Immediately, do whatever it takes to stop intrusion activity, if it still occurring and determine the nature, extent and details of the intrusion.
- Determine notification requirements.
    - Consumers will be notified if their Personal Identifiable Information has been exposed. If we identify that the data breach was contained to a few consumers, (e.g., less than 10 consumers), we will notify the consumer by phone. If the intrusion was more extensive, consumers will be mailed a letter providing details and that contains our toll-free number. o Prepare/Approve Notification.

- The President, in consultation with the Information Technology Manager and legal counsel will prepare and approve the notification—whether the actual communication is via, telephone or postal mail.

- Debrief with the President, IT Manager and any other involved individuals and/or Human Resources to prevent future occurrences.

(See Appendix B. Page 10 Deverus Technology)

Stored Data Security Models

- Stored Data Security (In House-Outsourced Platform)

S2Verify's policy is to ensure backup data is encrypted, and stored in a locked location.

Our procedure is to entrust all backups to our software platform vendor. We do not locally backup.

Our software platform vendor has certified that all of our backup data is encrypted and stored in a secure facility.

(See Appendix B, Page 8, Deverus Technology)

Consumer Protection

Password Protocol Models

- Password Protocol Policy and Procedure Language

S2Verify's policy is to issue unique usernames to each employee for each system the employee is authorized to access, to require the use of a strong password (a minimum of six (6) characters), and to require that each password be changed at least once every 120 days. Employees agree to treat passwords as confidential information and are prohibited from writing them down or sharing them with any other individual, inside or outside of the company. Our employee who is responsible for password protocol securely maintains records of issuance.

Our procedure is to periodically review this policy with each employee and confirm their understanding. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

- Employee Handbook Language or Addendum Language

The protection of consumer information is a critical component of your employment with S2Verify.

S2Verify issues unique usernames to each employee for each system the employee is authorized to access, requires the use of a strong password (a minimum of six (6) characters), and requires that each password be changed at least once every 120 days.

As a condition of employment, you agree to treat passwords as confidential information and are prohibited from writing them down or sharing them with any other individual, inside or outside of the company.

Your supervisor will periodically review this policy with you and confirm your understanding. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

(See Appendix B, Page 10 Deverus Technology for full Password Protocol)

Electronic Access Control Model

• Electronic Access Control Policy and Procedure Language

S2Verify's policy is to grant access to consumer information to employees only if required by their job function and then limit access to only that needed to perform their job. We have evaluated each department's needs and categorized the access rights needed within each department according to job classification.

When an employee is hired, promoted, demoted or transferred, the employee's supervisor for the new position approves access parameters required by the job. The employee's former supervisor (if applicable) is responsible for ensuring the former employee's access is disabled. (Upon employment termination, the former employee's access/password to all S2Verify systems are disabled as part of the termination process.) The process is for the employee's supervisor to request permission/disabling to our employee who is responsible for password protocol and securely maintains records of issuance and disabling as detailed in our 1.5 Password Protocol.

S2Verify's policy is to issue unique usernames to each employee for each system the employee is authorized to access, to require the use of a strong password (a minimum of six (6) characters), and to require that each password be changed at least once every 120 days. Employees agree to treat passwords as confidential information and are prohibited from writing them down or sharing them with any other individual, inside or outside of the company. Our employee who is responsible for password protocol securely maintains records of issuance.

When necessary, vendors are granted access using strong passwords, but only to the areas needed to perform their function and then only to the specific information needed to perform their function.

Clients are required to use strong passwords, these passwords are required to be changed every 120 days and we allow client users to assign unique access rights for their employees.

(See Appendix A, Section 1.6 Policy and Procedure Manuel for full Electronic Access Control)

Physical Security Model

- Physical Security Policy and Procedure Language

S2Verify has a physical security policy to control access to areas containing consumer information.

S2Verify Personnel
Employees are issued key fab and/or key and only has access to areas in which they are authorized by management to perform their job. The supervisor of the individual will authorize additional access upon hire or a change in job assignment.

S2Verify Visitors/Guests/Vendors
All visitors moving beyond our reception area must sign a registry upon arrival and are checked out upon departure. The registry contains the date, person they wish to see, reason for visit and time of arrival/departure.

Visitors may be granted approval to web access using their own laptop or other device for the purposes of checking email or getting on the internet. However, under no circumstances will visitors be granted access to any employee's log-in credentials or other means that would enable them to access consumer information.

While on the premises, visitors shall be escorted at any time when consumer information is available on computer screens, hard copy or electronic media of any type.

S2Verify Temporary/Contract Workers
Temporary or contract workers are, as rule, not granted access to areas that contain consumer information that is not locked in a secure location. If a temporary or contract worker is considered for a position requiring access to a secure areas, they must first undergo the due diligence and make the same certifications as an employee would.

(See Appendix A, Section 1.7 Policy and Procedure Manual for Full Electronic Access Control)

Consumer Information Privacy Policy Model

Consumer Information Privacy Policy

S2Verify is a consumer reporting agency. It is required by the Fair Credit Reporting Act, 15 U.S.C. §1681 *et seq.* ("FCRA") to maintain the confidentiality of all consumer information.

S2Verify obtains information on an individual consumer only upon the request of a user who has a permissible purpose under the FCRA to request information on that consumer in order to provide consumer reports. The FCRA requires a user for employment purposes to certify to us that it has a permissible purpose for the report and has obtained the written consent of the consumer to request information before we can supply the requested information.1 The user must submit to reasonable audits by us to confirm that it is, in fact, obtaining such consents. All users must certify that they have a permissible purpose to request a report such as credit, insurance, and renting an apartment. Our customers agree to keep your information confidential and secure.

S2Verify does not maintain a database of consumer information.

Personal Information Disclosure, United States or overseas. We do not send consumer information outside of the United States or its territories for any purpose other than to deliver a report to an end user. Of course, if information is sought from outside of the United States, the information is gathered in that country and then transmitted to us here in the United States where it is treated as any other consumer information.

Any information gathered on any consumer may only be provided to the user authorized by the consumer or permitted by the FCRA or similar state law to receive the information. We cannot and do not share, sell or distribute consumer information with or to any third party other than the requesting party thereof. Any consumer, upon proper identification, has the right under the FCRA to request us to furnish to the consumer any and all information we may have on that consumer. The consumer has the right to dispute the accuracy or completeness of any information contained in the consumer's file. However, we may be required, upon receipt of a court order to release the information in civil litigation, or as otherwise required by law, to disclose information regarding a consumer to law enforcement agencies.

.
If you have any questions regarding our policy, you may contact our Chief Privacy Officer at:

Email: Jim.Zimbardi@s2verify.com

Telephone: 855-671-1933

Mailing Address: P.O. Box 2587, Roswell, GA 30077

Other privacy initiatives and procedures include, but are not limited to:

- Access to confidential consumer information is limited within S2Verify to those who have a need to know the information: obtaining and transmitting information on the consumer or those dealing with a consumer request for information or consumer disputes.
- Access to S2Verify computer terminals, file cabinets, fax machines, trash bins, desktops, etc. are secure from unauthorized access.
- S2Verify maintains a secure network to safeguard consumer information from internal and external threat.
- All backup data is maintained in an encrypted form.
- S2Verify maintains records on each request for information and identifies each user who requested information on a consumer.
- Employees are prohibited from "browsing" files or databases without a business justification.
- Destruction of consumer information follows the Federal Trade Commission's requirements that the information be unreadable upon disposal.

(See Appendix B, Deverus Technology for full Information Security)
(See Appendix C, Employee Handbook Addendum for full Employee Policy on Consumer Information)

Unauthorized Browsing Models

• Unauthorized Browsing Policy and Procedure Language

S2Verify policy prohibits employees from browsing files and databases for any reason outside of their need to perform their essential job functions.

Appropriate use of browsing files or databases is strictly limited to legitimate business purposes. Inappropriate browsing includes searching on family members, acquaintances, public figures, politicians—in fact anyone not associated with your specific employment functions.

Employees are informed of this policy in the Employee Handbook and Policy and Procedure Manual. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

- Employee Handbook Unauthorized Browsing Language or Addendum Language

Employees are prohibited from browsing files and databases for any reason outside of those needed to perform essential job functions. Appropriate use of browsing files or databases is strictly limited to legitimate business purposes. Inappropriate browsing includes searching on family members, acquaintances, public figures, politicians—in fact anyone not associated with your specific employment functions. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

(See Appendix C, Employee Handbook Addendum Section 1.9)

Record Destruction Models

- Data Destruction Policy and Procedure Language (Outsource)

S2Verify has a professional document destruction firm to destroy/render inaccessible/unreadable and or unrecoverable all consumer and client information per current FTC rules. Prior to using this firm, we performed due diligence to insure their competence.

Our procedure is to put all paper files of any type that contain consumer information in secure, locked bins for the destruction firm to pick up. Our employees are instructed to lock up any files containing consumer information every day prior to the conclusion of their work day.

While not done in the normal course of business, any consumer information that is in an electronic file of any type is erased or destroyed

at the immediate conclusion of the task associated with it, but never left unlocked at the end of the work day.

- Employee Handbook Language or Addendum Language;

The protection of consumer information is a critical component of your employment with S2Verify.

S2Verify has a record destruction policy and procedure that requires you to ensure that any consumer information you work with be destroyed. It is critical that you follow our authorized procedures, but also *never* leave any paper or electronic records at your workstation containing consumer information unless they are under lock and key prior to you leaving after your work day.

(See Appendix C, Section 1.10 of Employee Handbook Addendum)

Consumer Disputes Model

- Consumer Disputes Policy and Procedure Language

Consumer Dispute Policy and Procedures

Overall Policy

In the course of providing information to our clients, we may receive communication from consumers disputing all, or part, of the information we have provided. Upon receipt of such a communication, our policy is to:

- At no charge to the consumer, re-investigate, confirm, correct and/or delete the disputed information within 30 days (45 days if extended) of our receipt of the notice of the dispute.
- Notify the information provider of the dispute with 5 days of receipt.
- The consumer advocate representative handling the dispute will consider the information provided by the consumer. If the consumer advocate representative

believes the dispute is frivolous or irrelevant, the representative should speak with their supervisor. If the supervisor agrees, legal counsel will be consulted and the consumer will be so advised.

- Upon conclusion of the re-investigation, the appropriate parties, e.g., consumer, vendor, employer, client, will be notified and the consumer shall be informed of our re-investigation process upon request.

Consumer Dispute Procedures

Any employee receiving a communication from a consumer disputing, or questioning information on a report, should immediately forward the communication to a consumer advocate. If by phone, do not dispute what the consumer says or get into the details—transfer the call to the consumer advocate, their voice mail or take a message.

Consumer Advocate Procedures

1. Insure consumer identity.
   This is done by matching a minimum of two identifiers which may include full name, date of birth, SSN, current or previous addresses and/or driver's license number.
2. Explain the report and determine whether consumer is disputing the information or just had an interpretive question. If the consumer disputes all, or any part of the report:
3. Create a consumer file.
4. Notify the source of the information of the dispute, what was reported and what, exactly, is being disputed. This should be done immediately, but in no case less than 5 days from receipt. In exceptional cases, the consumer advocate believes the dispute is frivolous or irrelevant; if so, the representative should immediately notify their supervisor. If the supervisor disagrees, the investigation should proceed. If the supervisor agrees the dispute is frivolous or irrelevant, legal counsel should be consulted.
5. Investigate the information reported. The operative procedure in a dispute is to go to the original source/repository of the information—not necessarily the source from whom we received the information. For example, if it is an employment history or reference, go back to the original source. If it is a criminal record, go back to the jurisdiction holding the record. If the jurisdiction was a state repository, go to the county jurisdiction. If the jurisdiction does not provide information remotely, use a different court retriever and order the same information. If the consumer disputes information contained on a driving record, contact the state Department of Motor Vehicles.
6. Investigatory steps taken should be documented. This includes the source, person if available, date contacted, information requested and information received. All information should be retained in the consumer file.

7. Upon conclusion of the investigation, a determination is made as to whether the original information is correct, partially incorrect/incomplete or all incorrect/unable to verify.
8. If the original information is determined to be correct, the consumer is notified. If the information is partially incorrect/incomplete, the consumer, client and source (including vendor/original retriever if applicable) are notified and supplied a corrected report. If the original report was incorrect in total, a correct report is provided to the consumer, client and source (if applicable). If a corrected report is unavailable, for example the original source is out of business, the consumer and client are notified of this fact. The client should be notified to consider the original report unverified and check with their legal counsel.
9. All of this determination information, actions taken/new information sent should be documented and/or retained in the consumer file. Consumer files are securely retained for a minimum of three years.
10. In addition, if a determination is made that the original information reported was incorrect in whole, or part, it is the responsibility of the representative to report to their supervisor the facts, judgment on the cause of the mistake and suggestion for future prevention of the same mistake. This includes, but is not limited to a training change/re-emphasis or personnel action with employees, increased monitoring or dismissal of court retrievers/vendors or system procedures. The consumer representative supervisor should present these recommendations to their supervisor, management or take action as required to prevent future occurrences.

(See Appendix A, Section 1.11 Policy and Procedure Manual for full Consumer Disputes policy)

Sensitive Data Masking Model

• Sensitive Data Masking Policy and Procedure Language

S2Verify policy is to suppress the entire SSN in any form outside our company unless the information is required by the client/vendor, allowed by law and securely transported. Specifically, SSNs are suppressed to any entity outside our firm unless:

1. The full SSN is required to perform the search requested (e.g., employment verification) **or**
2. The full SSN is demanded to be returned by the client **and**,

    a. The disclosure is not prohibited by law **and**
    b. The data is limited to that which is needed **and**
    c. Secure transport methods (Policy and Procedures 1.2 and 4.5) are used.

3. The full SSN is never sent via US standard mail. The whole number is suppressed or if requested by the client, the last 4 digits will be shown.

Our policy regarding other sensitive data is similar. Specifically,

4. We do not send out a full name with either the DOB or driver license number unless it is required by the client/vendor and securely transported (Policy and Procedure 1.2 and 4.5).

Our procedure is to set up each client and vendor template to not send the SSN/Name and DOB or DL number unless approved by appropriate supervisory permission.

(See Appendix A, Section 1.12 Policy and Procedure Manual or full Sensitive Data Masking)

Database Criminal Records Model

- Database Criminal Records Policy and Procedure Language

S2Verify adjudicates all records that contain hits, which means a physical person reviews all charges and convictions for efficacy, accuracy and report-ability based on Federal and State laws and client criteria.

Database record currency is reviewed by the President and Compliance Officer.

S2Verify orders county and or state search to verify the information contained in the Database file.

(See Appendix A, Section 1.13 Policy and Procedure Manual for full Database Criminal Records)