



SAGE DIRECT, INC. PRIVACY POLICY AND INFORMATION SAFEGUARD PLAN

Sage Direct, Inc. recognizes the sensitive nature of our customer's information and the information of their members/clients and/or customers. We protect the privacy of this information and the way that this information is used. This Privacy Policy and Information Safeguard Plan outlines the way in which Sage Direct, Inc. protects the confidentiality of this information and our security standards for handling this information. The President and Owners of Sage Direct, Inc. are responsible for the enforcement of this Policy.

The Types Of Customer Information Sage Direct Obtains

Sage Direct, Inc. hereafter referred to as "the Company", provides statement processing and direct marketing services for its customers that may contain account numbers, social security numbers, account balances, account transactions and addresses ("Customer Information").

How Do We Use Customer Information?

We will not disclose any Customer Information to any organization or entity, affiliated or non-affiliated, unless this disclosure is necessary to initiate, administer, or enforce a transaction or service for which we have been contracted to perform.

How Do We Keep Customer Information Private?

We take steps to safeguard Customer Information. We maintain physical, electronic and procedural safeguards to guard the information against unauthorized access. We also utilize appropriate corrective action when needed to enforce employee compliance with our procedures with regard to privacy of information.

Procedural Safeguards

1. Only the Company's employees that have received training (described below) are authorized to receive or make phone calls to discuss Customer Information.
2. The Company is only authorized to request validation of information. Company procedures state responsibilities and confidentiality responsibilities of each associate.
3. All contract service vendors with access to Customer Information are required to supply their Privacy Policy and/or Information Safeguard Plans to the Company prior to providing services for the Company. These policies are reviewed to determine compliance and appropriate safeguards. However, under no circumstance should this paragraph be deemed to create a representation, guaranty or any duty by the Company relating to the safeguarding of Customer Information by third parties.

Physical Safeguards

1. Sage has fire alarms and extinguishers throughout the building. ADP monitors the fire alarm system. The fire department and the owners will be notified in the event of a fire. The staff has been trained in the proper use of both the fire alarm system and the extinguishers.
2. All Customer Information is kept in restricted office areas and is only available to authorized employees.
3. Any Customer Information that needs to be disposed of is placed in locked shred bins located in the restricted areas within the Company. The Company's personnel lock these bins during all office non-business hours.

4. All paper statements produced from the customer data are either placed directly by employees or vendors in the United States Mail or are placed in locked shred bins if they cannot be mailed for some reason. No paper copies of statements are maintained.

Information System Safeguards

1. All Customer statement information (not including eStatements) is maintained on our computer system for no more than 31 days.
2. Clients of customers who have opted for eStatements can access their own information on the network through the use of a password. This Customer information is stored solely on a secure network server and is deleted after no more than three statement cycles, which can be monthly, quarterly or annually.
3. Any hardware that is no longer in use has the memory and all programs erased and are destroyed by a qualified computer technician.
4. The system information is backed up by using magnetic media. This back up occurs weekly and monthly. All monthly back up media is stored at a secure location offsite.
5. All computers are protected with anti-virus software, which is updated on a daily basis and renewed annually. In addition, inbound and outbound e-mails are scanned prior to reaching the e-mail recipient's destination. All internal networks are isolated from outside intrusion via Firewalls. The FTP server only allows access to two directories, incoming and outgoing. They are both blind directories, which means anyone outside of the internal network will not "see" any files in these directories. Any files containing personal information deposited in the incoming directory are required to be encrypted and password protected. Passwords are sent separately via e-mail.

Employee Hiring and Training

1. Security background checks are performed on all full-time employees that have access to financial data that is processed and/or printed at the Company. No employee is hired that has been convicted of a felony. Employees with background checks will be considered to have full security clearance to work on financial data and/or printed statements. These employees are trained to monitor part-time staff without the same level of security clearance. Part time employees never perform work on financial data files and do not have access to computers that have this information or any other customer information on them. The work part time employees perform on printed statements is monitored at all times by full time staff with full security clearance.
2. Each employee is required to review the Company's Privacy Policy upon commencing employment. The employee is required to sign an acknowledgement that he/she has read, understands and will enforce the policy.
3. Each employee is required to attend a privacy training session that is presented by a Manager of the Company once per year.
4. The training includes a review of the Privacy Policy. The Company's procedures are reviewed so that each individual understands his/her role in protecting Customer Information. Each employee is informed of what information may be provided and to whom. If there is any doubt in the employee's mind, a Manager is to be consulted.
5. Employees are required to verify any request for Customer Information in order to be certain that the person requesting the information has the right to receive it. This may be done by validating the phone number of the caller or knowing the caller. In the event this cannot be done, the employee is instructed to return the call to insure that the phone number is appropriate to the company or individual requesting the information. In any case, the

owner of the data will be informed of the request and written permission will be required if the information is going to a third party.

6. Employees are also trained in recognizing any fraudulent attempt to obtain Customer Information and the steps to take in the event fraudulent attempts are identified. A Manager is informed of the possible attempt and is to notify our Customer and the appropriate law enforcement agency in the event the attempt is confirmed.

Our Conduct upon Discovery of Unauthorized Access

In the event we discover that there has been any form of unauthorized access to Customer Information we will immediately advise our Customer of such unauthorized access so that it can expeditiously implement its response program to such unauthorized disclosure as set forth in the Interagency Guidelines Establishing Information Security Standards pursuant to Section 505(b) of the Gramm–Leach–Bliley Act.