# Customer Information Security Policy

**Revision Date: 5/26/2021**

## 1. Overview

The Gramm-Leach-Bliley Act (GLBA), its implementing regulation – Regulation P, and the Standards for Safeguarding Customer Information (Safeguards Rule) provide standard for protecting borrower information. Under the GLBA and Regulation P, financial institutions are required to provide notices to their customers about their information-sharing practices and explain to customers their right to "opt out" if customers do not want their information shared with certain third parties. Under the Safeguards Rule, financial institutions must protect the consumer information they collect and to have measures in place to keep customer information secure.

## 2. Definitions

The following definitions apply for this Policy. They are not intended to be a complete list of official definitions under GLBA or the Safeguards Rule.

- **Customer Information** – means any record containing nonpublic personal information (NPI) about a customer of a financial institution, whether in paper, electronic, or other form, that is handled or maintained by or on behalf of Asertaloans or any affiliates, if applicable.
- **Information Security Program** – means the administrative, technical, or physical safeguards Asertaloans uses to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle customer information.
- **Nonpublic Personal Information (NPI)** – means any personally identifiable financial information that a financial institution collects about an individual in connection with providing a financial product or service, unless that information is otherwise publicly available. NPI includes:
    - any information an individual gives Asertaloans to get a loan (for example, name, address, income, Social Security number, or other information on an application);
    - any information about an individual that results from a transaction involving Asertaloans' financial product(s) or service(s) (for example, the fact that an individual is a consumer or customer, account numbers, payment history, loan or deposit balances, and credit or debit card purchases); or
    - any information Asertaloans gets about an individual in connection with providing a financial product or service (for example, information from court records or from a consumer report).

  NPI does not include information that Asertaloans has a reasonable basis to believe is lawfully made "publicly available." In other words, information is not NPI when Asertaloans has taken steps to determine:
    - that the information is generally made lawfully available to the public; and
    - that the individual can direct that it not be made public and has not done so.

- **Service Provider** – means any person or entity that receives, maintains, processes, or otherwise is permitted access to customer information through its provision of services directly to a financial institution.

## 3. Policy Statement

Asertaloans has adopted this Customer Information Security Policy (CIS Policy) designed to protect customer information, including administrative, technical, and physical safeguards used by Asertaloans to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle customer information. In developing the CIS Policy, Asertaloans has considered its size and complexity, the nature and scope of its activities, and the sensitivity of any customer information at issue.

The objectives of customer information security are designed to:

- Ensure the security and confidentiality of customer information.
- Protect against any anticipated threats or hazards to the security or integrity of customer information.
- Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

There are many critical elements of the CIS Policy, including assigning accountability, assessing risk, continuing training and education, developing internal controls, testing and monitoring, overseeing service providers, and planning for future developments.

## 4. Assigning Accountability

Under the Safeguards Rule, Asertaloans must designate an employee to coordinate an information security program. This employee will have the necessary knowledge, expertise, and authority to oversee implementation of information security requirements. Asertaloans has designated the Chief Information Security Officer to be responsible for maintaining and updating the information security program.

## 5. Assessment of Risk

Asertaloans must identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks.

### A. Company Risk Profile

Asertaloans is a non-depository financial institution engaged in the mortgage industry. Taking into account the systems and controls in place, Asertaloans believes that it has an overall risk profile that is moderate. The risks Asertaloans may encounter include:

- Unauthorized access of information by someone other than the customer
- Compromised information system security as a result of system access by a computer hacker
- Interception of data during transmission
- Loss of data integrity
- Physical loss of data in a disaster
- Errors introduced into the system
- Corruption of data or systems

- Lack of transaction completeness and documentation
- Unauthorized access of information by employees
- Unauthorized telephone requests for information
- Unauthorized access through hardcopy files or reports
- Unauthorized transfer of information through third parties

Asertaloans recognizes that this may not be a complete list of the risks associated with the protection of customer information. Since technology growth is not static, new risks are created regularly. Asertaloans plans to take the necessary steps to identify internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer records.

## 6. Employee Management and Training

Asertaloans realizes that information security depends largely upon its employees. Asertaloans will provide its employees with training (either in person or through written materials) regarding Asertaloans' policies and procedures for safeguarding customer information. Asertaloans will track employee attendance and will retain training materials and attendance records for audit and examination purposes.

To ensure proper safeguards, Asertaloans will also implement practices which may include but are not limited to:

- Checking references or obtaining background checks before hiring employees who may have access to customer information.
- Providing employees with training, policies and procedures for safeguarding customer information and requiring employees to acknowledge that they will comply with confidentiality and security standards for handling customer information.
- Limiting access to customer information to those employees who have a business need to see it. Preventing terminated employees from accessing sensitive information by immediately deactivating their passwords and user names and taking appropriate measures.
- Controlling access to customer information by requiring employees to use “strong” passwords that must be changed on a regular basis. Strong passwords include at least six characters, upper- and lower-case letters, and a combination of letters, numbers and symbols.
- Using password-activated screen savers to lock employee computers after a period of inactivity.
- Developing policies for appropriate use and protection of laptops, PDAs, cell phones, or other mobile devices.
- Training employees to take basic steps to maintain the security, confidentiality, and integrity of customer information, including:
    - Locking rooms and file cabinets where records are kept;
    - Not sharing or openly posting employee passwords in work areas;
    - Encrypting sensitive customer information when it is transmitted electronically via public networks;
    - Referring calls or other requests for customer information to designated individuals who have been trained in how Asertaloans safeguards personal data;

  - Reporting suspicious attempts to obtain customer information to designated personnel, including reporting on “pretext callers” who pretend to be the customer to obtain further customer information.

- Regularly reminding employees of Asertaloans' policy, and the legal requirement, to keep customer information secure and confidential.
- Developing safeguarding policies for employees who telecommute and requiring employees to use protections against viruses, spyware, and other unauthorized intrusions.
- Imposing disciplinary measures for security policy violations.

## 7. Information Systems

Information systems include the following: network and software designs, information processing, storage, transmission, and disposal. Asertaloans will implement practices to maintain security throughout the life cycle of customer information, from data entry to data disposal.

### A. Securely Storing Customer Information

Asertaloans appreciates the importance of knowing where sensitive customer information is stored, that it is stored securely, and that only authorized employees have access to it. To ensure proper safeguards, Asertaloans will implement practices which may include but are not limited to:

- Ensuring that storage areas are protected against destruction or damage from physical hazards, such as fire, floods or earthquakes.
- Storing records in a room or cabinet that is locked when unattended.
- Ensuring that a server or computer where customer information is stored is accessible only with a “strong” password and is kept in a physically-secure area.
- Avoiding storing sensitive customer information on a computer with an internet connection, where possible.
- Maintaining secure backup records and keeping archived data secure by storing it off-line and in a physically-secure area.
- Maintaining a careful inventory of computers and other equipment which contains customer information.

### B. Secure Transmission of Customer Information

Customer information must be transmitted in a secure manner. Asertaloans will take proper steps to ensure secure transmission of customer information, which may include but are not limited to the following:

- When credit card information or other sensitive financial data is transmitted, a Secure Sockets Layer (SSL) or other secure connection is used to protect the information in transit.
- If information is collected online directly from customers, the transmission should automatically be secure. In addition, customers should be cautioned against transmitting sensitive data via email or in response to an unsolicited email or pop-up message.
- If sensitive data must be transmitted by email over the Internet, the data must be properly encrypted.

### C. Disposal of Customer Information

Asertaloans requires that customer information be disposed of in a secure manner and consistent with the FTC's Disposal Rule, where applicable. Employees are required to shred any papers containing customer information so that the information cannot be reviewed or reconstructed. In addition, Asertaloans and its employees must destroy or erase data when disposing of computers, disks, CDs, magnetic tapes, hard drives, laptops, PDAs, cell phones, or any other electronic media or hardware which contains customer information.

## 8. Protecting Against Security Breaches

Asertaloans must deter, detect, and defend against attacks, intrusions, or other system failures. Asertaloans will take reasonable steps to prevent attacks, quickly diagnose a security incident, and have a plan in place for responding effectively if a breach occurs.

### A. Monitoring Websites Failure to Secure Customer Information

Asertaloans will monitor the websites and communications of its software vendors to learn of emerging threats and available updates or other defenses to protect against these threats. In addition, Asertaloans will read relevant industry publications or news about potential threats and available defenses.

### B. Maintain Up-To-Date Programs and Controls

Asertaloans will maintain appropriate programs and controls that are up-to-date to prevent unauthorized access to customer information. In doing so, Asertaloans will:

- check with software vendors regularly to obtain and install patches or updates that resolve software vulnerabilities;
- use anti-virus and anti-spyware software that automatically updates;
- maintain firewalls that are up-to-date;
- regularly review ports that are not used for business to ensure they are closed; and
- promptly provide information and instruction to employees on new security risks or potential breaches.

### C. Detect Improper Disclosure or Theft of Customer Information

Asertaloans must have appropriate procedures to detect the improper disclosure or theft of customer information. Procedures may include:

- keeping logs of activity about the network and monitoring them for signs of unauthorized access to customer information;
- using an up-to-date intrusion detection system to alert of attacks;
- monitoring both in-bound and out-bound transfers of information for potential breaches; and
- inserting a dummy account into each customer list and then monitoring the account to detect any unauthorized contacts or charges.

### D. Steps in the Event of a Breach

Asertaloans will take steps to preserve the security, confidentiality, and integrity of customer information if a breach occurs by:

- taking immediate action to secure any information that has or may have been compromised;
- preserving and reviewing files or programs that might review how the breach occurred;
- bringing in security professionals to help assess the breach as soon as possible, if feasible and appropriate; and
- notifying customers of the security breach as required by state or federal laws.

### E. Notifications

In the case of a security breach, Asertaloans will perform an investigation to determine which customers' personal information was subject to the breach and whether those customers should be informed of the security breach. Asertaloans will also determine if it should notify law enforcement if the breach may involve criminal activity, identity theft, or related harm and whether credit bureaus or other businesses that may be affected by the breach should be notified. Asertaloans will comply with state laws when making the foregoing determinations.

## 9. Overseeing Service Providers

In conducting its business, Asertaloans relies on various service providers. Asertaloans will take reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for customer information. Asertaloans will require service providers by contract to implement and maintain appropriate measures to safeguard customer information and to refrain from sharing any customer information with other parties. Asertaloans will review and adjust contracts as necessary to obligate service providers to implement appropriate measures designed to meet the objectives of the GLBA and the Safeguards Rule.

## 10. Evaluating and Adjusting the Information Security Needs

Asertaloans will evaluate and adjust its information security needs based on the results of the testing and monitoring it performs. In addition, Asertaloans will make appropriate adjustments in light of any material changes to its operations or business, or for any other circumstances that may have a material impact on the security of customer information. Asertaloans will assess, document, and mitigate current and new risks to its information security program at least annually.