# Acra Lending – Standards for Safeguarding Customer Information

## Table of Contents

# Section 1 – Introduction

The Federal Trade Commission, (the "FTC"), has issued a final rule, as posted in the Federal Register on May 23, 2002, creating regulation 16CFR, Part 314, *Standards for Safeguarding Customer Information,* as required by section 501(b) of the Gramm-Leach-Bliley Act also known as the "Privacy Act".

This regulation went into effect on May 23, 2003 and affects a wide range of entities, including, but not limited to: non-depository lenders; consumer reporting agencies; debt collectors; data processors; courier services; retailers that extend credit by issuing credit cards to consumers; personal property or real estate appraisers; check-cashing businesses; mortgage brokers, and any other entity that meets this definition.

This regulation requires all financial institutions to develop, implement and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to the size and complexity of the entity, the nature and scope of its activities, and the sensitivity of any customer information at issue.

# Section 2 – General Requirements

The regulation requires all financial institutions to develop, implement, and maintain a comprehensive information security program, which contains certain general elements.

These general elements require all financial institutions to:

1. Designate an employee or employees to coordinate its customer information security program in order to ensure accountability and achieve adequate safeguards.
2. 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.
3. To consider risks in each area of its operations, including three specific areas of concern:
4. Checking references and/or performing background checks before hiring employees who will have access to customer information.
5. Preventing terminated employees from accessing customer information by immediately deactivating usernames and passwords.
6. Employee training and management such as:
    a. Locking rooms and filing cabinets where records are stored
    b. Not sharing or openly posting passwords in work areas
    c. Encrypting sensitive customer information that is transmitted electronically by any means when containing Non-Public Personal Information ("NPPI")
    d. Reporting suspicious attempts to obtain customer information.
7. Limiting access to customer information to only those employees who have a business reason to see it.
8. Establish information systems protocols that include information processing, storage, transmission and disposal (in accordance with the Disposal Rule)
9. Using password-activate screen savers to lock employee computers after periods of inactivity.
10. Detecting, preventing, and responding to attacks, intrusions, or other systems failures.
11. Monitoring the websites of software vendors and reading relevant industry publications for news about emerging threats and available defenses against them.
12. Design and implement customer information safeguards to control the identified risks through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems and procedures.

13. To take reasonable steps to assure itself that its current and potential service providers maintain sufficient procedures to discover and respond to widely-known security failures by its current and potential service providers.
14. To evaluate and adjust its customer information security program in light of the results of the testing and monitoring of its written standards or any material changes to its operations or business arrangements, or any other circumstances that are known or become known that have a material impact on its customer information security program

# Section 3 – Designation of Security Coordinator

As required by regulation 16 CFR, Part 314, *Standards for Safeguarding Customer Information*, Acra Lending is designating its **Compliance Officer** to coordinate the customer information security program to ensure accountability and achieve adequate safeguards.

# Section 4 – Minimizing Risks

## Internal Risks

It is the policy of Acra Lending to protect and secure any and all non-public and personal information regarding our customers, employees, and business relationships. Acra Lending will continue to make every effort to ensure non-public and personal information of our customers, employees, and business relationships and secure internally by following the standards set forth below:

1. Employees are required to sign an agreement to follow Acra Lending's confidentiality and security standards for handling customer information.
2. Employees are required to lock computers when workstation is unoccupied and use password-activated screen savers to lock computers after a period of inactivity.
3. Employees are required not to leave individual pieces of documentation unsecured on their desk or any other place or location. Make sure documentation is secured inside a file or filing cabinet at all times.
4. Employees are required not to leave loan files, employee records or business relationship files sitting open and unattended on a desk or any other place or location for extended periods of time. Printouts should be immediately removed from the printer and if applicable disposed in an official shredder bin.
5. Employees are required not to leave loan files, employee records or business relationship files out and open on a desk overnight. Make sure loan files, employee records or business relationship files are closed and put away in a desk or filing cabinet before you leave for the day.
6. Employees are not permitted to ever give "employment references", Human Resources will handle all employment verifications. "Company" and "Credit References" refer these phone calls, fax or mail requests to management.
7. All papers MUST be cleared, stored, or shredded at end of business day to ensure that any sensitive documents are not left in printer trays for wrong person to pick up.
8. Treat mass storage devices such as optical, hard, or USB drives as sensitive and secure them in a locked drawer or room.
9. Employees are expected to verify the identity of any caller wishing to discuss loan information, and confirm the requestor has authority to discuss loan information.
10. Employees are not allowed to provide non-public / personal information to third parties without written authorization from the subject person or business entity.
11. Employees working remotely must adhere to the following:
    a. Establish a defined designated workspace within the employee home

b. Ensure assigned IT equipment is set up correctly.
c. Establish defined security measures to ensure workspace is secure.
d. Use a secure Wi-Fi network and take the appropriate steps to ensure router is secure.
e. Install all Acra Lending required updates as prescribed.
f. Save all data on designated share drive or work computer (or as instructed)
g. Do not use Acra Lending issued equipment for personal use
h. Do not install any ancillary devices on Acra Lending's issued computer.
i. Disconnect from VPN connection and turn off the Acra Lending issued computer when workday is complete.
j. All email communications containing Non-Public Personal Information (NPPI), internal or external, are to be sent securely using Acra Lending's email encryption.

12. Employees that work on a Mobile basis must adhere to the following:
    a. Nonuse of company logos or name will be saved on screen saver or computer wall paper
    b. Shall not conduct business calls that disclose company or customer personal information in areas where information can be heard by the public.
    c. Employee will be responsible for proper storage and accounting of equipment when traveling.
    d. Use of public internet is prohibited.
    e. Accessing or using third party networks for internet is prohibited.
    f. Employee will ensure they block sigh lines when accessing company or customer personal information in public.

## External Risks

It is the policy of Acra Lending to protect and secure any and all non-public and personal information regarding our customers, employees and business relationships.

Acra Lending will continue to make every effort to ensure non-public and personal information of our customers, employees, and business relationships are secure externally by following the standards set forth below:

1. Acra Lending requires all borrower electronically transmitted information and communication to comply with Company's Electronic Communication Consent Agreement.
2. Acra Lending requires encryption of sensitive customer information when it is transmitted electronically and is not under the purview of Company's Electronic Communication Consent Agreement.
3. All calls or other request for customer information to designated individuals who have been trained in how your company safeguards personal data.
4. Any documentation including, but not limited to, the following information is to be placed in "shred" bins:
    a. Social Security Numbers
    b. Names and Addresses
    c. Property or Mailing Addresses
    d. Loan Numbers
    e. Bank Account Numbers
    f. Credit Card Numbers
    g. Employer's names, addresses or phone numbers
    h. Credit status or history
    i. Employment status or history
    j. Corporate Proprietary Information

# Section 5 – Employee Training

It is the policy of Acra Lending to protect and secure any and all non-public and personal information regarding our customers, employees and business relationships.

Acra Lending will continue to make every effort to ensure non-public and personal information of our customers, employees and business relationships are secure by ensuring all personnel are trained on the importance of having and following safeguard standards.

All personnel will be given a copy of our Standards for Safeguarding Customer Information by the Human Resources Department upon hire.

All personnel will also be required to take the following designated security training at hire and yearly thereafter.

1. SSCI & Safeguarding Company Information

Upon assignment, all personnel will be instructed by their supervisors on our standards for securing non-public/personal information of our customers, employees and business relationships.

Acra Lending's standards for securing non-public/personal information of our customers, employees and business relationships will be reviewed with all personnel annually, at the time of the annual employee review.

# Section 6 – Service Provider Compliance with Standards

As required by regulation 16 CFR, Part 314, Standards for Safeguarding Customer Information, Acra Lending will take reasonable steps to assure that our current and potential service providers maintain sufficient procedures to detect and respond to security breaches and that we will maintain reasonable procedures to discover and respond to widely known security failures by our current and potential service providers.

See Acra Lending's Vendor Management Program policy for additional details.

# Section 7 – Reporting Security Breaches

It is the policy of Acra Lending to protect and secure any and all non-public and personal information regarding our customers, employees and business relationships.

Acra Lending will continue to make every effort to ensure non-public and personal information of our customers, employees and business relationships are secure however, sometimes unauthorized disclosure, misuse, alteration, destruction or other compromise of such information can occur.

Any personnel who sees or is made aware of any non-compliance with our standards, unauthorized disclosure, misuse, alteration, destruction or other compromise of any nonpublic/personal information regarding a customer, employee or business relationship, by Acra Lending personnel, a service provider or by any outside source, must report it, as soon as possible, to a Acra Lending manager or supervisor.

The Acra Lending manager or supervisor should take the report to Senior Management and an investigation should be implemented immediately to ascertain the extent of the breach and what steps should be taken to

minimize the exposure to the customer, employee or business relationship.

If Acra Lending personnel committed the breach, there will be swift and proportional disciplinary action taken, including, but not limited to being verbally warned, written up and/or terminated. If a service provider committed the breach, the contract with that service provider will provide for a premature cancellation of the contract due to said breach. If an outside source committed the breach, the customer, employee, or business relationship will be contacted and informed of the breach, so that they may take whatever steps they feel necessary.

See Acra Lending's Information Technology Security Program for additional details.

## Section 8 – Monitoring Compliance with Security

As required by regulation 16 CFR, Part 314, Standards for Safeguarding Customer Information, Acra Lending has designated its Compliance Officer to coordinate the customer information security program and monitor the effectiveness of the safeguards and standards through observation and examination.

The Compliance Officer will verify compliance with this policy through various methods, including but not limited to, periodic walk-throughs, business tool reports, and internal/external audits.

The Compliance Officer will validate with the Human Resources department that all personnel are given a copy of our Standards for Safeguarding Customer Information at hire.

The Compliance Officer will validate with the managers and supervisors at Acra Lending that they are aware of our standards, as set forth in the Standards for Safeguarding Customer Information, and are going over it with all personnel at first assignment and during the annual review process.

The Compliance Officer will validate with the Legal Department that the Service Provider contracts contain verbiage certifying that they have implemented and maintain the required safeguards and standards as set forth in 16 CFR, Part 314.

All managers and supervisors at Acra Lending, in particular, the Compliance Officer, will pay close attention to individual conversations and actions in regards to loan files, employee records and business relationship files to ensure that nothing is left loose or left out and that non-public/personal information is not being disclosed without the proper authorizations and to individuals with a "need- to-know".

# Section 9 – Acknowledgement Page

I hereby acknowledge and certify that I have received, read, and understand Acra Lending's Standards for Safeguarding Customer Information Policy.

I also hereby acknowledge and certify that I will follow the standards as set forth in this policy to safeguard customer information.

As a manager or supervisor of Acra Lending, I also hereby Acknowledge and certify that I will make available to my staff, the necessary tools to follow the standards as set forth in the policy and will regularly go over the standards to ensure understanding and compliance.

| | |
|---|---|
| Printed Name | Position |
| Signature | Date |

**THIS PAGE IS TO BE COMPLETED AND FILED IN THE EMPLOYEES PERSONNEL FILE FOR FUTURE REFERENCE.**

| Revision Date | Details | Compliance Approved |
|---|---|---|
| 5/24/2020 | Formatting and grammar corrections | |
| 8/12/2020 | Email encryption, policy change | 8/12/20 |
| 8/13/2020 | Added NPPI verbiage | 8/13/20 |
| 3/10/2021 | Revised NPPI verbiage | 3/10/21 |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |