CITADEL
SERVICING CORPORATION

CSC – Standards for Safeguarding Customer Information

Table of Contents

SECTION 1 - INTRODUCTION 2

SECTION 2 – GENERAL REQUIREMENTS 2

SECTION 3 – DESIGNATION OF SECURITY COORDINATOR 3

SECTION 4 – MINIMIZING RISKS: 3

A. Internal Risks 3

B. External 4

SECTION 5 – EMPLOYEE TRAINING 5

SECTION 6 – SERVICE PROVIDER COMPLIANCE WITH STANDARDS 5

SECTION 7 – REPORTING SECURITY BREACHES 5

SECTION 7 – MONITORING COMPLIANCE WITH SECURITY 6

SECTION 7 – MONITORING COMPLIANCE WITH SECURITY 6

A. ACKNOWLEDGEMENT PAGE 6

CITADEL
SERVICING CORPORATION

CSC – Standards for Safeguarding Customer Information

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-LeachBliley 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:

a) Designate an employee or employees to coordinate its customer information security program in order to ensure accountability and achieve adequate safeguards.

b) 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.

c) To consider risks in each area of its operations, including three specific areas of concern:

   1. Employee training and management;
   2. Information systems, including information processing, storage, transmission and disposal; and
   3. Detecting, preventing and responding to attacks, intrusions, or other systems failures.

d) 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.

e) To take reasonable steps to assure itself that its current and potential service providers maintain sufficient procedures to detect and respond to security breaches, and maintain reasonable procedures to discover and respond to widely-

known security failures by its current and potential service providers.

f) 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*, CSC is designating its **Compliance Officer** to coordinate the customer information security program to ensure accountability and achieve adequate safeguards.

SECTION 4 – MINIMIZING RISKS:

A. Internal Risks

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

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

a) Employees are required to sign an agreement to follow CSC's confidentiality and security standards for handling customer information.

b) Employees are required to lock computers when workstation is unoccupied and use password-activated screen savers to lock computers after a period of inactivity.

c) 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.

d) Employees are required not to leave loan files, employee records or business relationship files sitting open and unattended on your 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.

e) Employees are required not to leave loan files, employee records or business relationship files out and open on your desk overnight. Make sure loan files, employee records or business relationship files are closed and put away in desk or file cabinet before you leave for the day.

f) 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.

g) 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 .

h) Treat mass storage devices such as optical, hard, or USB drives as sensitive and secure them in a locked drawer or room.

i) Employees are expected to know at all times to whom they are speaking to on the telephone and/or who is requesting non-public/personal information, make the

requestor identify themselves. Make sure the requestor has a "need-to-know", but never provide any non-public/personal information about a customer, employee or business relationship. If the requestor requires a confirmation of information; 1) make sure you are knowledgeable and authorized to verify that information, and then 2) only answer with a "yes" or "no". All other information requests shall be in writing.

B. External

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

CSC 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:

a) CSC requires all borrower electronically transmitted information and communication to comply with CSC's Electronic Communication Consent Agreement.

b) CSC requires encryption of sensitive customer information when it is transmitted electronically via public networks and is not under the purview of CSC's Electronic Communication Consent Agreement.

c) All calls or other requests for customer information to designated individuals who have been trained in how your company safeguards personal data.

d) Any documentation including, but not limiting, 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

Any documentation or forms containing this type of non-public/personal information shall only be placed in the "shred" bins, to be picked up by a professional disposal company. These "shred" bins shall be placed throughout the building and made readily available to all personnel.

CSC – Standards for Safeguarding Customer Information

SECTION 5 – EMPLOYEE TRAINING

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

CSC 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.

Upon assignment, all personnel will be instructed by their individual supervisors on our standards for securing non-public/personal information of our customers, employees and business relationships. These standards can be found on page 5 through 7 of this manual, under the section "Minimizing Risks".

Our 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,* CSC 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.

SECTION 7 – REPORTING SECURITY BREACHES

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

CSC 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 CSC personnel, a service provider or by any outside source, must report it, as soon as possible, to a CSC manager or supervisor.

The CSC 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 CSC 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.

SECTION 7 – MONITORING COMPLIANCE WITH SECURITY

As required by regulation 16 CFR, Part 314, *Standards for Safeguarding Customer Information*, CSC 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 no limited to, periodic walk-thrus, 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 CSC 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 CSC, 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 7 – MONITORING COMPLIANCE WITH SECURITY

A. ACKNOWLEDGEMENT PAGE

I hereby acknowledge and certify that I have received, read and understand CSC'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 CSC, 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.