

Table of Contents

TABLE OF CONTENTS	2
SECTION 1 GENERAL	4
1.1 STATEMENT OF PURPOSE.....	4
1.2 OBJECTIVE	4
1.3 STATE LAW AND AGENCY GUIDELINES	4
SECTION 2 SUMMARY	5
2.1 PRIVACY OF CONSUMER FINANCIAL INFORMATION	5
2.1.1 Coverage	5
2.2 FEDERAL TRADE COMMISSION STANDARDS FOR SAFEGUARDING CUSTOMER INFORMATION	5
2.2.1 Coverage	5
SECTION 3 REQUIREMENTS	6
3.1 INITIAL PRIVACY NOTICE TO CUSTOMERS AND CONSUMERS	6
3.1.1 Existing Customers.....	6
3.2 ANNUAL PRIVACY NOTICE TO CUSTOMERS.....	7
3.3 REQUIRED CONTENT FOR PRIVACY NOTICES.....	7
3.3.1 Short-Form Initial Notice with Opt-Out Notice for Non-Customers.....	8
3.3.2 Form of Opt-Out Notices and Opt-Out Methods.....	9
3.3.3 Model Privacy Forms	9
3.3.4 Opt-Out Notice Delivered Subsequent to Initial Notice	9
3.4 CONSUMERS OPT-OUT DIRECTION	9
3.5 REVISED PRIVACY NOTICES.....	9
3.6 DELIVERING PRIVACY AND OPT-OUT NOTICES.....	10
3.6.1 Electronic Delivery of Privacy and Opt-Out Notices	10
3.7 EXCEPTIONS.....	12
3.7.1 Exceptions for Service Providers and Joint Marketing	12
3.7.2 Exceptions for Processing and Servicing Transactions	12
3.7.3 Other Exceptions	12
3.7.4 Exceptions for Annual Notice.....	13
3.8 SAFEGUARDS RULE	14
3.8.1 Prohibited Activities	16
3.8.2 Permitted Use of Licensed Software	16
3.8.3 Passwords and Access Codes	17
3.8.4 Requirements for Firewall.....	17
3.8.5 Controlled Access.....	18
3.8.6 Clean Desk Enforcement.....	18
3.8.7 Proper Document Destruction	18
SECTION 4 ORIGATION COMPLIANCE	20
4.1 INITIAL PRIVACY DISCLOSURE	20
SECTION 5 SERVICING COMPLIANCE	21
5.1 INITIAL PRIVACY NOTICE.....	21
5.2 ANNUAL PRIVACY NOTICE	21
5.3 CUSTOMERS OPT-OUT DIRECTION	21
SECTION 6 RECORD RETENTION	23
APPENDIX 1 DEFINITIONS	24

APPENDIX 2 REFERENCE LIST 28

Sample

Section 2 Summary

2.1 Privacy of Consumer Financial Information

Privacy of Consumer Financial Information (Regulation P) requires financial institutions to provide certain privacy notices and to comply with certain limitations on the disclosure of [nonpublic personal information](#) to [nonaffiliated third parties](#) and requires financial institutions and others to comply with certain limitations on redisclosure and reuse.

2.1.1 Coverage

Regulation P applies only to nonpublic personal information about individuals who obtain financial products or services primarily for personal, family, or household purposes, from institutions and other persons for which the CFPB has rulemaking authority, including third parties that are not financial institutions but that receive nonpublic personal information from financial institutions with whom they are not [affiliated](#).

2.2 Federal Trade Commission Standards for Safeguarding Customer Information

The Safeguards Rule, issued by the Federal Trade Commission as part of the implementation of the Gramm-Leach-Bliley Act (GLBA), requires all financial institutions under the jurisdiction of the FTC to have measures in place to securely protect [customer](#) information. Institutions must develop their own safeguards for protecting [consumer](#) information and must ensure that their affiliates and service providers also have safeguards in place around customer information.

2.2.1 Coverage

The Safeguards Rule applies to financial institutions subject to FTC jurisdiction and that are not subject to the enforcement authority of another regulator under Section 505 of the GLBA, including, for purposes of this guide, mortgage lenders, mortgage brokers, and non-federally insured credit unions.

3.8.1 Prohibited Activities

Employees are prohibited from using [Sample Client]'s e-mail system, network, or internet/intranet access for the following activities:

- Downloading software without the prior written approval from [Sample Client]
- Printing or distributing [Sample Client]'s or any other copyrighted materials including, but not limited to, software, articles, and graphics protected by copyright
- Using software that is not licensed by the manufacturer or approved by [Sample Client]
- Sending, printing, or otherwise disseminating [Sample Client]'s proprietary data, or any other information deemed confidential by [Sample Client] to unauthorized persons
- Operating a business or otherwise engaging in commercial activity outside the scope of employment unless prior permission to do so is obtained
- Sending or forwarding messages containing a consumer's credit or confidential information or account numbers
- Sending or forwarding a message that discloses personal information without [Sample Client]'s authorization including accessing, transmitting, receiving, or seeking confidential information about borrowers or mortgage transactions without authorization
- Using another employee's password or impersonating another person while communicating or accessing [Sample Client]'s network or the internet

3.8.2 Permitted Use of Licensed Software

[Sample Client] regularly purchases, leases, or maintains site licenses for computer software applications from a variety of commercial manufacturers. To ensure compliance with software license agreements and [Sample Client]'s information security policy, employees must adhere to the following:

- Employees must use software in accordance with the manufacturer's license agreements and [Sample Client]'s policy. Employees acknowledge they do not own software or its related documentation. Employees may not make additional copies of software, unless expressly authorized by the software publisher.
- Any employee who knowingly makes, acquires, or uses unauthorized copies of computer software licensed to [Sample Client], or who places or uses unauthorized software on [Sample Client]'s premises or equipment is subject to disciplinary action or termination.
- Employees must obtain permission from [Sample Client] prior to installing personal software on [Sample Client]'s computer system. Employees are not permitted to copy software from [Sample Client]'s computer system for installation on home or other computers without prior authorization.

Appendix 1 Definitions

Affiliate

Any company that controls, is controlled by, or is under common control with another company. In the case of a federal credit union, a credit union service organization (CUSO) that is controlled by the federal credit union is an affiliate. Additionally, an affiliate of a federally-insured, state-chartered credit union is a company that is controlled by the credit union

Board of Directors

An executive committee that supervises the activities of an organization. As it relates to a Compliance Management System (CMS), the board is ultimately responsible for developing and administering a CMS that ensures compliance with federal consumer financial laws and addresses and minimizes associated risks of harm to consumers. In a non-depository consumer financial services company, that ultimate responsibility may rest with a board of directors in the case of a corporation or with a controlling person or some other arrangement. Some institutions may be governed by firm-wide standards, policies, and procedures developed by a holding company or other top-tier corporation for adoption, use, and modification, as necessary, by subsidiary entities.

Clear and Conspicuous

Readily understandable. In the case of written and electronic disclosures, the location and type size must be readily noticeable and legible to consumers, although no minimum type size is mandated. In the case of oral disclosures, the disclosures must be given at a volume and speed sufficient for the consumer to hear and comprehend them.

Compliance Management System (CMS)

A comprehensive system that drives an institution's compliance responsibilities; communicates those responsibilities to employees; ensures that responsibilities for meeting legal requirements and internal policies and procedures are incorporated into business processes; reviews operations to ensure responsibilities are carried out and legal requirements are met; and takes corrective action and updates tools, systems, and materials, as necessary.