Table of Contents

TABLE OF CONTENTS 1
CHAPTER 1 INTRODUCTION 4
1.1 GOALS AND OBJECTIVES 4
1.2 REQUIRED REVIEW 4
1.3 APPLICABILITY 4
1.4 ROLE AND RESPONSIBILITIES OF THE COMPLIANCE OFFICER 5
1.5 ROLE AND RESPONSIBILITIES OF THE EXECUTIVE BOARD 5
1.6 LEGAL REQUIREMENTS OF SECTIONS 114 AND 315 OF FACTA 6
CHAPTER 2 MONITORING AND QUALITY CONTROL 7
2.1 INTERNAL CONTROLS 7
2.2 QUALITY CONTROL 8
2.3 AUDITING 8
2.4 BOARD/SENIOR MANAGEMENT OVERSIGHT 8
CHAPTER 3 STAFF AND TRAINING 9
3.1 ONGOING TRAINING 9
3.2 NEW HIRE TRAINING 10
3.3 TRAINING PROTOCOLS 10
CHAPTER 4 OVERVIEW OF [SAMPLE CLIENT]'S RED FLAGS IDENTITY THEFT PLAN 11
4.1 SUMMARY 11
4.2 IDENTIFYING INFORMATION 11
4.3 DEFINITIONS 11
4.4 IDENTIFICATION OF RED FLAGS 13
4.5 LIST OF RED FLAGS FROM THE FEDERAL TRADE COMMISSION 14
CHAPTER 5 RED FLAG DETECTION AND RESPONSE 16
5.1 ADDRESS DISCREPANCIES 16
5.2 ACCURACY OF INFORMATION FROM CREDIT AGENCY REPORTS 16
5.3 SOCIAL SECURITY VALIDATION 16
5.4 FACTUAL ID REPORTS 17
5.5 FRAUD CHECKS 17
5.6 ALERTS, WARNINGS FROM A CONSUMER REPORTING AGENCY 17
5.7 PROCEDURES FOR MITIGATING ALERTS FROM A CREDIT AGENCY 18
5.8 PRESENTATION OF SUSPICIOUS DOCUMENTS 18
5.9 PRESENTATION OF SUSPICIOUS PERSONAL IDENTIFYING INFORMATION 18
5.10 NOTICES RECEIVED FOR SUSPICIOUS ACTIVITY 19
5.11 RED FLAG RESPONSE TO PRESENTED DOCUMENTS 19

5.12 REPOLLUTION OF A BORROWER'S CREDIT REPORT 20

CHAPTER 6 MITIGATION 21

6.1 ASSESSMENT OF RISK 21
6.2 MITIGATION STEPS FOR CLEARED VARIANCE 21
6.3 NONRETURNING PREQUALIFICATION APPLICANTS 21
6.4 STEPS WHEN THE RED FLAG CANNOT BE MITIGATED 22
6.5 FILING A SUSPICIOUS ACTIVITY REPORT 22
6.6 IDENTITY THEFT AFFIDAVIT 23

CHAPTER 7 INFORMATION SECURITY 24

7.1 SAFEGUARDING CONFIDENTIAL INFORMATION 24
7.2 HOW INFORMATION IS OBTAINED 24
7.3 EMAIL POLICIES AND PROCEDURES 25
7.4 ELECTRONIC ACCESS 26
7.5 NETWORK AND INTERNET POLICY 27
7.6 SOCIAL MEDIA 27

7.6.1 Risk Management 28
7.6.2 Regulatory Compliance 29

7.7 PROHIBITED ACTIVITIES 29
7.8 AUTHORIZED USE OF SOFTWARE 30
7.9 ADMINISTRATIVE ACCESS CONTROL 31
7.10 FIREWALL PROCEDURES 31
7.11 DATA CENTER SECURITY 32
7.12 DOCUMENT DESTRUCTION 32
7.13 INCIDENT RESPONSE AND PREPAREDNESS 33

CHAPTER 8 CONSUMER PRIVACY 34

8.1 PRIVACY POLICY 34
8.2 GRAMM-LEACH-BLILEY ACT 34
8.3 CONSUMER PRIVACY NOTICE TO APPLICANTS 34
8.4 CONFIDENTIALITY AGREEMENT FOR SERVICE PROVIDERS 35
8.5 CLOSING AGENT AUTHORITY UNDER THE CONSUMER PRIVACY ACT 35

CHAPTER 9 FAIR AND ACCURATE CREDIT TRANSACTIONS ACT 36

9.1 SUMMARY OF THE FAIR AND ACCURATE CREDIT TRANSACTIONS ACT 36
9.2 NOTICES REQUIRED UNDER FACTA 36
9.3 FRAUD ALERTS AND ACTIVE DUTY ALERTS—INITIAL ALERT 37
9.4 ACCESS TO FREE REPORTS—INITIAL ALERT 38
9.5 FRAUD ALERT AND ACTIVE DUTY ALERT – EXTENDED ALERT 38
9.6 ACCESS TO FREE REPORTS—EXTENDED ALERT 38

CHAPTER 10 FAIR CREDIT REPORTING ACT 40

10.1 SUMMARY OF THE REGULATION 40
10.2 PERMISSIBLE PURPOSE 40
10.3 CREDIT OR INSURANCE SOLICITATIONS 41
10.4 RESPONSIBILITIES OF FURNISHERS OF INFORMATION 41
10.5 RESPONSIBILITIES REGARDING DISPUTES 42
10.6 RECORD RETENTION 42

CHAPTER 11 USA PATRIOT ACT 43

11.1 CUSTOMER IDENTIFICATION PROGRAM 43
11.2 CUSTOMERS SUBJECT TO CIP REQUIREMENTS 43
11.3 REQUIRED CUSTOMER INFORMATION TO BE COLLECTED 43
11.3.1 Required Customer Information for U.S. Persons 43
11.3.2 Required Customer Information for Non-U.S. Customers 44
11.4 VERIFICATION THROUGH DOCUMENTS 45
11.5 CUSTOMER NOTICE 45
11.6 RECORD RETENTION 45

CHAPTER 12 ECONOMIC GROWTH, REGULATORY RELIEF, AND CONSUMER PROTECTION ACT 46
CHAPTER 13 VENDOR MANAGEMENT 47

13.1 POLICY STATEMENT 47
13.2 VENDOR RISK ASSESSMENT 47
13.3 VENDOR MONITORING 48

CHAPTER 14 RED FLAGS CHECKLIST 49

14.1 MORTGAGE RED FLAGS CHECKLIST 49

Chapter 5 Red Flag Detection and Response

5.1 Address Discrepancies

[Sample Client] requires immediate response to all notices of address discrepancy that are received from the credit reporting agency. The notice is sent when the agency has noted a substantial difference between the borrower's address the company provided when requesting the report, and the address in the agency's file.

Upon receipt of such notice, it is the responsibility of the loan processor or underwriter to compare the information in the credit report provided by the agency and verify the information in the credit report directly with the consumer.

[Sample Client] is required by law to furnish a borrower's address to the credit agency after the processor or underwriter reasonably confirms accuracy to the credit agency. Reasonable confirmation occurs when [Sample Client]

- can form a reasonable belief that the credit report relates to the borrower;
- has established a continuing relationship with the borrower, and
- regularly furnishes information to the credit agency.

5.2 Accuracy of Information from Credit Agency Reports

[Sample Client] requires that all credit reports and additional investigative reports be cross referenced for accuracy. Should there be a discrepancy in a borrower's address or other identifying information from one consumer report to an additional report, all steps and procedures must be followed. The response, request for borrower explanations, and other mitigation must be separately applied to each consumer report ordered. [Sample Client] must inform applicants that they can dispute the accuracy of credit information directly through the credit reporting agency.

5.3 Social Security Validation

[Sample Client] requires a Social Security validation from a minimum of at least one consumer credit agency or factual investigation service. No mortgage file can continue with processing based on the Social Security number that is provided on employer wage statements or other identifying information. Validation of the Social Security number must be from authorized sources that obtain information from the Social Security Administration.

Chapter 6 Mitigation

6.1 Assessment of Risk

[Sample Client] must assess the level of risk and evaluate the exposure to identity theft to the company and/or consumer. All processors and underwriters must immediately respond to suspicious activities, bogus or suspicious documents, document discrepancies, alerts on the credit report, and/or alerts or warnings on a fraud check or Factual ID. The employee must respond to the Red Flag on a level that is commensurate with the degree of risk posed to the borrower or company. In some cases, the risk may be increased due to identity theft caused by a data security breach.

6.2 Mitigation Steps for Cleared Variance

[Sample Client] must proceed with proper steps for mitigating the Red Flag or alert. These steps are followed when a Red Flag is cleared due to circumstances where there is a bona fide error or explained variance:

1. Contact the customer to obtain explanations and/or documentation.
2. Contact employers, gift donors, or financial institutions to correct or supplement erroneous information previously provided.
3. Update the information on the reported loan application and LOS system.
4. Update the credit report via an interactive comment/feedback option.
5. Update the documents contained in the loan file.
6. Complete the Red Flag Checklist.

6.3 Nonreturning Prequalification Applicants

[Sample Client] must proceed with proper steps for mitigating the Red Flag or alert for all loan applications, including pre-qualifications that do not result in a submitted application, an application closed for incompleteness, a denied application, and withdrawn application. These steps are followed when a Red Flag is detected:

1. Complete the Red Flag Checklist.
2. Issue a letter to the consumer that describes the Red Flag and a statement that informs the applicant that, due to the cancellation of the application, the lender is not responsible for further steps that may be required to correct or mitigate the discrepant data

Chapter 11 USA PATRIOT Act

[Sample Client] must comply with Section 326 of the Act of Congress known as the USA PATRIOT Act, officially entitled the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act, which establishes minimum standards for a financial institution's customer identification program (CIP).

11.1 Customer Identification Program

These requirements relate to the identification and verification of any person who applies to open an account. The CIP requires lenders to establish procedures which include, but are not limited to, the following actions:

- Verifying the identity of any person seeking to open an account to the extent reasonable and practicable
- Maintaining records of the information used to verify the person's identity including name, address, and other identifying information
- Determining whether the person appears on any lists of known or suspected terrorists or terrorist organizations provided to the financial institution by any government agency

11.2 Customers Subject to CIP Requirements

Under the USA PATRIOT Act, customers who are subject to CIP requirements include the following:

- A person who opens a new account
- An individual who opens a new account for
  - another individual who lacks legal capacity, such as a minor; or
  - an entity that is not a legal person, such as a civic club.

11.3 Required Customer Information to Be Collected

11.3.1 Required Customer Information for U.S. Persons

At a minimum, the rules require that the company obtain the following information from a U.S. person (U.S. citizens, U.S. registered corporations, partnerships, or trusts) prior to opening an account:

- Name