ETANA CUSTODY
RED FLAG IDENTITY THEFT PREVENTION PROGRAM
NOVEMBER 10, 2022

This section outlines the Bank's Identity Theft Prevention Program approved by the Board of Directors of **Etana Custody (Etana)** on **November 10, 2022**.

This Program includes:

H. Customer Notification for Suspected Identity Theft
I. Identity Theft Affidavit

VIII. DEFINITIONS

I. POLICY DESCRIPTION, OBJECTICE, AUTHORITY AND SCOPE

It is the policy of **Etana** to comply with the intent of all provisions of the program by establishing this policy as the Bank's written policy and compliance program. The objective is to develop a written Identity Theft Prevention Program, designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account.

All employees of **Etana**, herein referenced to as the "Bank", shall comply with the terms of this program immediately. All officers and employees shall modify system configurations and procedures, if necessary, to comply with the terms of this policy. The Identity Theft Program Compliance Program is formally approved by the Board of Directors and will be approved annually or before if any revisions are made to the program. Changes in operating procedures, standards, guidelines and technologies, provided they are consistent with this program, may be authorized by the Compliance Officer.

No part of this program or its supporting operating procedures should be interpreted as contravening or superseding any other legal and regulatory requirements placed upon **Etana.** Protective measures should not impede other legally mandated processes such as records retention or subpoenas. Any conflicts should be submitted immediately to the Compliance Officer for further evaluation and/or subsequent submission to the Bank's management.

Requests for exceptions to this program must be very specific and may only be granted on specific items, rather than to entire sections, request are to be submitting by an internal memorandum to the Compliance Officer for consideration by Senior Management.

NOTE: All officers of the Bank are responsible for the comprehension and implementation of this program and ensuring their employees understanding of their responsibilities. If at any time an employee is uncertain about the proper method of handling a situation or transaction, he or she should refer the issue to their immediate supervisor or contact the Compliance Officer for further clarification.

A. **Responsibility** - The ultimate responsibility of maintaining an effective Identity Theft Prevention Program is assigned to the Board of Directors. The Board of Directors will be responsible for the appointment of an Identity Theft Prevention Coordinator. The Identity Theft Prevention Coordinator will report to the Board of Directors. The Identity Theft Prevention Coordinator will work closely with the Bank's senior management and front-line personnel to identify, detect, and respond to appropriate Red Flags. All Bank employees are responsible for compliance with all Identity Theft Program requirements outlined in this policy.

B. **Accountability** – The Board of Directors has charged Senior Management with the responsibility to determine the necessary course of action to ensure adherence to appropriate

C. laws, regulations and is being managed in an effective and consistent manner for the entire organization.

Specifically, the Board of Directors is responsible for:

a. Ensuring the quality of the Bank's Identity Theft Program;

b. Designating a qualified Compliance Officer who is responsible for the oversight, development, implementation and administration of the Identity Theft Program;

c. Maintaining a working knowledge of the Bank's Identity Theft Program; and

d. Reviewing for formal adoption this and other related written policies and procedural guidelines necessary to ensure effective adherence with applicable compliance laws and regulations.

D. **Identity Theft Coordinator (Officer)** – Senior Management through the directive issued by the Board of Directors has elected **(Employee Name, Title)** to serve as the Identity Theft Officer, and to supervise the overall management of the Bank's Identity Theft Program. The Identity Theft Officer shall report directly to the Board of Directors and be dully approved by the Board of Directors. On at least an annual basis, the Identity Theft Officer is to make a written report to the Board of Directors regarding the status of the Bank's compliance activities with respect to the Identity Theft Program.

Specifically, the Identity Theft Officer is responsible for:

a. Performing all required risk assessments and provide a report to Senior Management;

b. Developing, implementing and maintaining detailed identity theft recordkeeping procedures;

c. Reviewing any related Bank policies and procedures to ensure compliance with the Bank's Identity Theft Program;

d. Training Bank personnel on Identity Theft Program directives;

e. Exercise appropriate and effective oversight of service provider arrangements; and

f. Supporting an independent Identity Theft Program audit program.

E. **Compliance Committee** – The Compliance Committee is to provide assistance to and support the Compliance Officer to promote effective management of the Bank's Identity Theft Program.
Specifically, the Compliance Committee is responsible for:

a. Assisting the Compliance Officer in ensuring the compliance mandate established by this policy is an integral part of Bank operations;

b. Ensuring the Board of Directors is informed of the Bank's compliance efforts on a periodic basis;

c. Providing guidance to the Compliance Officer to ensure the Bank adapts to changes mandated by the law;

d. Reviewing and approving the Bank's Identity Theft Program;

e. Providing assistance to the Compliance Officer with the responses to audit exceptions and/or regulatory examination results; and

f. Providing overall general guidance and expertise to ensure the successful implementation of the Bank's Identity Theft Program.

II. STATEMENT OF NEED AND DEFINITION

Etana is responsible for protecting personal and nonpublic information, which is gathered and stored in internal records for our customers. Regulatory agencies are charged with the responsibility to ensure financial institutions and creditors information security controls and procedures are in compliance with the intent of the regulations to protect a customer's identity. It is crucial for management and staff to understand the basic security requirements and provide ongoing assistance in detection, prevention and mitigation of identity theft to our customers.

This Identity Theft Prevention Program is designed to emphasize compliance with all information security requirements, including those detailed in the regulatory agency guidelines. Specifically, the intent of the Identity Theft Prevention Program is to meet the objectives of the FACT Act, as

set forth in OCC Rules and Regulations Subpart J of 12 CFR Part 41 – Identity Theft Red Flags and FDIC's Fair Credit Reporting Act guidelines. Furthermore, the Identity Theft Prevention Program is aligned with FFIEC requirements.

The Bank has established an Identity Theft Prevention Program that is designed to detect, prevent and mitigate identity theft in connection with the opening of a covered account or any existing covered account. This program is based on the Bank's nature and scope of its activities and includes policies and procedures to:

a. Identify relevant red flags for the covered accounts that the Bank offers or maintains, and incorporate those red flags into the program;

b. Detect red flags that have been incorporated into the program;

c. Respond appropriately to any red flags that are detected to prevent and mitigate identity theft; and

d. Ensure the program (including the red flags determined to be relevant) is updated periodically to reflect changes in risks to customers and to the safety and soundness of the Bank from identity theft.

In addition, the program ensures that the Bank adheres to other related legal requirements that may be applicable, such as:

a. The filing of Suspicious Activity Reports in accordance with applicable law and regulation;

b. Implementing any requirements regarding the circumstances under which credit may be extended when the Bank detects a fraud or active duty alert;

c. Implementing any requirements for furnishers of information to consumer reporting agencies, such as to correct or update inaccurate or incomplete information, and not to report information that the furnisher has reasonable cause to believe is inaccurate; and

d. Complying with the prohibitions regarding the sale, transfer and placement for collection of certain debts resulting from identity theft.

As such, the Board of Directors has approved this program and is required to review and reapprove the program (and related reports) on an annual basis thereafter. It is the responsibility of the Identity Theft Officer, Compliance Committee and Senior Management to:

a. Administer the program;

b. Exercise appropriate and effective oversight of service provider arrangements that engage a vendor to perform an activity in connection with one or more accounts to ensure that the activity of the service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent and mitigate the risk of identity theft in accordance with this policy and the Bank's Vendor Management Program Policy. As an example, the Bank may require a service provider to maintain appropriate policies and procedures to detect relevant red flags that may arise in the performance of the vendor's activities, and either report the red flags to the Bank or to take appropriate steps to prevent or mitigate identity theft;

c. Train Bank personnel as necessary to effectively implement the program; and

d. Provide the Board of Directors on at least an annual basis with a report that addresses material matters related to the program and evaluate such issues as the effectiveness of this and other related policies and procedures in addressing the risk of identity theft in connection with:

    1. The opening of accounts and existing accounts;

    2. Service provider arrangements;

    3. Significant incidents involving identity theft and management's response; and

    4. Recommendations for material changes to the program.

The program (including the red flags determined to be relevant) is to be periodically updated to reflect changes in risks to customers or to the safety and soundness of the Bank from identity theft, based on factors such as:

a. The experiences of the Bank with identity theft;

b. Changes in methods of identity theft;

c. Changes in methods to detect, prevent and mitigate identity theft;

d. Changes in the types of accounts that the Bank offers or maintains; and

e. Changes in the business arrangements of the Bank, including mergers, acquisitions, alliances, joint ventures and service provider arrangements.

III. IDENTIFICATION OF RED FLAGS

A. **Risk Factors** – To identify relevant Red Flags, **Etana** has evaluated the following factors.

a. Types of covered accounts – Etana offers the following types of covered accounts:

1. Cash management
2. Credit Accounts
3. Custodian services
4. Deposit Accounts
5. Lending Accounts
6. Safety deposit boxes or other safekeeping services
7. Trust Services

b. Methods to open a covered account – Etana requires in person.

c. Methods to access a covered account – Etana requires in person.

d. Previous experiences with identity theft - Etana will take into account previous experiences with identity theft when defining and updating Red Flags.

B. **Risk Matrix** –

Covered Account	Threat	Methods	Controls (Red Flags)	Likelihood	Potential Damage	Risk
Cash Management	Opened Fraudulently	In person	Address or Telephone Number Flags, Application Appears to be Altered or Forged, Consumer Report Address Discrepancy, Consumer Report Alert, Consumer Report Credit Freeze, Consumer Report Unusual Activity Pattern, Documents Altered or Forged, Incomplete Application, Information on ID Inconsistent with Information on File,	Medium	Major	High

			Information on ID Inconsistent with Information Provided, Personal ID Associated with Known Fraudulent Activity, Personal ID is Inconsistent with External Information, Personal ID is Inconsistent with Information on File, Personal ID is Inconsistent with Other Personal ID, Personal ID is of a Type Common to Fraudulent Activity, Photograph or Physical Description Inconsistency, The SSN has been Submitted by Other Persons			
Cash Management	Unauthorized Access	In person	Customer is not Receiving Account Statements, Account Use is Inconsistent with Normal Activity, Challenge Question Responses Unavailable or Limited, Documents Altered or Forged, Inactive Account is Used, Information on ID Inconsistent with Information on File, Information on ID Inconsistent with Information Provided, Key Changes Shortly After Change of Address, Mail is Returned on an Active Account, Notice that a Fraudulent Account has been Opened, Notification of Unauthorized Changes or Transactions, Personal ID is Inconsistent with Information on File, Photograph or Physical Description Inconsistency	Medium	Major	High

Credit Accounts	Opened Fraudulently	In person	Address or Telephone Number Flags, Application Appears to be Altered or Forged, Consumer Report Address Discrepancy, Consumer Report Alert, Consumer Report Credit Freeze, Consumer Report Unusual Activity Pattern, Documents Altered or Forged, Incomplete Application, Information on ID Inconsistent with Information on File, Information on ID Inconsistent with Information Provided, Personal ID Associated with Known Fraudulent Activity, Personal ID is Inconsistent with External Information, Personal ID is Inconsistent with Information on File, Personal ID is Inconsistent with Other Personal ID, Personal ID is of a Type Common to Fraudulent Activity, Photograph or Physical Description Inconsistency, The SSN has been Submitted by Other Persons	Medium	Major	High
Credit Accounts	Unauthorized Access	In person	Customer is not Receiving Account Statements, Account Use is Inconsistent with Normal Activity, Challenge Question Responses Unavailable or Limited, Documents Altered or Forged, Inactive Account is Used, Information on ID Inconsistent with Information on File,	Medium	Major	High

			Information on ID Inconsistent with Information Provided, Key Changes Shortly After Change of Address, Mail is Returned on an Active Account, New Revolving Credit Account Follows Fraud Patterns, Notice that a Fraudulent Account has been Opened, Notification of Unauthorized Changes or Transactions, Personal ID is Inconsistent with Information on File, Photograph or Physical Description Inconsistency			
Custodian services	Opened Fraudulently	In person	Address or Telephone Number Flags, Application Appears to be Altered or Forged, Consumer Report Address Discrepancy, Consumer Report Alert, Consumer Report Credit Freeze, Consumer Report Unusual Activity Pattern, Documents Altered or Forged, Incomplete Application, Information on ID Inconsistent with Information on File, Information on ID Inconsistent with Information Provided, Personal ID Associated with Known Fraudulent Activity, Personal ID is Inconsistent with External Information, Personal ID is Inconsistent with Information on File, Personal ID is Inconsistent with Other Personal ID, Personal ID is of a Type Common to Fraudulent Activity, Photograph or	Medium	Major	High

			Physical Description Inconsistency, The SSN has been Submitted by Other Persons			
Custodian services	Unauthorized Access	In person	Customer is not Receiving Account Statements, Account Use is Inconsistent with Normal Activity, Challenge Question Responses Unavailable or Limited, Documents Altered or Forged, Inactive Account is Used, Information on ID Inconsistent with Information on File, Information on ID Inconsistent with Information Provided, Key Changes Shortly After Change of Address, Mail is Returned on an Active Account, Notice that a Fraudulent Account has been Opened, Notification of Unauthorized Changes or Transactions, Personal ID is Inconsistent with Information on File, Photograph or Physical Description Inconsistency	Medium	Major	High
Deposit Accounts	Opened Fraudulently	In person	Address or Telephone Number Flags, Application Appears to be Altered or Forged, Consumer Report Address Discrepancy, Consumer Report Alert, Consumer Report Credit Freeze, Consumer Report Unusual Activity Pattern, Documents Altered or Forged, Incomplete Application, Information on ID Inconsistent with Information on File,	Medium	Major	High

			Information on ID Inconsistent with Information Provided, Personal ID Associated with Known Fraudulent Activity, Personal ID is Inconsistent with External Information, Personal ID is Inconsistent with Information on File, Personal ID is Inconsistent with Other Personal ID, Personal ID is of a Type Common to Fraudulent Activity, Photograph or Physical Description Inconsistency, The SSN has been Submitted by Other Persons			
Deposit Accounts	Unauthorized Access	In person	Customer is not Receiving Account Statements, Account Use is Inconsistent with Normal Activity, Challenge Question Responses Unavailable or Limited, Documents Altered or Forged, Inactive Account is Used, Information on ID Inconsistent with Information on File, Information on ID Inconsistent with Information Provided, Key Changes Shortly After Change of Address, Mail is Returned on an Active Account, Notice that a Fraudulent Account has been Opened, Notification of Unauthorized Changes or Transactions, Personal ID is Inconsistent with Information on File, Photograph or Physical Description Inconsistency	Medium	Major	High

Lending Accounts	Opened Fraudulently	In person	Address or Telephone Number Flags, Application Appears to be Altered or Forged, Consumer Report Address Discrepancy, Consumer Report Alert, Consumer Report Credit Freeze, Consumer Report Unusual Activity Pattern, Documents Altered or Forged, Incomplete Application, Information on ID Inconsistent with Information on File, Information on ID Inconsistent with Information Provided, Personal ID Associated with Known Fraudulent Activity, Personal ID is Inconsistent with External Information, Personal ID is Inconsistent with Information on File, Personal ID is Inconsistent with Other Personal ID, Personal ID is of a Type Common to Fraudulent Activity, Photograph or Physical Description Inconsistency, The SSN has been Submitted by Other Persons	Medium	Major	High
Lending Accounts	Unauthorized Access	In person	Customer is not Receiving Account Statements, Account Use is Inconsistent with Normal Activity, Challenge Question Responses Unavailable or Limited, Documents Altered or Forged, Inactive Account is Used, Information on ID Inconsistent with Information on File,	Medium	Major	High

			Information on ID Inconsistent with Information Provided, Key Changes Shortly After Change of Address, Mail is Returned on an Active Account, Notice that a Fraudulent Account has been Opened, Notification of Unauthorized Changes or Transactions, Personal ID is Inconsistent with Information on File, Photograph or Physical Description Inconsistency			
Safety deposit boxes or other safekeeping services	Opened Fraudulently	In person	Address or Telephone Number Flags, Application Appears to be Altered or Forged, Consumer Report Address Discrepancy, Consumer Report Alert, Consumer Report Credit Freeze, Consumer Report Unusual Activity Pattern, Documents Altered or Forged, Incomplete Application, Information on ID Inconsistent with Information on File, Information on ID Inconsistent with Information Provided, Personal ID Associated with Known Fraudulent Activity, Personal ID is Inconsistent with External Information, Personal ID is Inconsistent with Information on File, Personal ID is Inconsistent with Other Personal ID, Personal ID is of a Type Common to Fraudulent Activity, Photograph or Physical Description Inconsistency, The SSN has	Medium	Major	High

			been Submitted by Other Persons			
Safety deposit boxes or other safekeeping services	Unauthorized Access	In person	Customer is not Receiving Account Statements, Account Use is Inconsistent with Normal Activity, Challenge Question Responses Unavailable or Limited, Documents Altered or Forged, Inactive Account is Used, Information on ID Inconsistent with Information on File, Information on ID Inconsistent with Information Provided, Key Changes Shortly After Change of Address, Mail is Returned on an Active Account, Personal ID is Inconsistent with Information on File, Photograph or Physical Description Inconsistency	Medium	Major	High

C. **Sources of Red Flags** – The Bank will incorporate relevant Red Flags from sources such as:

   a. Incidents of identity theft **Etana** has experienced.

   b. Methods of identity theft that reflect changes in identity theft risks.

   c. Applicable supervisory guidance.

D. **Categories of Red Flags** – The Bank will categorize relevant Red Flags into the following categories:

   a. Alerts, notifications or other warnings received from consumer reporting agencies or service providers, such as fraud detection services.

   b. The presentation of suspicious documents.

c. The presentation of suspicious personal identifying information, such as a suspicious address change.

d. The unusual use of, or other suspicious activity related to, a covered account.

e. Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identify theft in connection with covered accounts held by the financial institution or creditor.

E. **Detecting Red Flags** – The Bank will address detection of Red Flags in connection with opening of covered accounts and existing covered accounts by:

a. Obtaining identifying information about, and verifying the identity of, a person opening a covered account. The Bank will use the policies and procedures regarding identification and verification set forth in the Customer Information Program (CIP), as defined in 31 U.S.C. 5318(l) (31 CFR 103.121).

b. Authenticating customers, monitoring transactions and verifying the validity of change of address requests, in the case of existing covered accounts.

F. **Preventing and Mitigating Red Flags** – The bank has measures in place to appropriately respond to Red Flags detected that are commensurate with the degree of risk posed.

Appropriate responses may include:

a. Monitoring a covered account for evidence of identity theft;

b. Contacting the customer;

c. Changing any passwords, security codes or other security devices that permit access to a covered account;

d. Reopening a covered account with a new account number;

e. Not opening a new covered account;

f. Closing an existing covered account;

g. Not attempting to collect on a covered account or not selling a covered account to a debt collector;

h. Notifying law enforcement; or

i. Determining that no response is warranted under the particular circumstances.

When determining the appropriate response, the Bank will consider aggravating factors that may heighten the risk of identity theft, such as a data security incident that results in unauthorized access to a customer's account records held by the Bank or a third party, or notice that a customer has provided information related to a covered account held by the Bank to someone fraudulently claiming to represent the bank or to a fraudulent website.

IV. REGULATORY REQUIREMENT

- 12 CFR Part 41 Subpart J (c) (Periodic Identification of Covered Accounts) states:
"Each financial institution or creditor must periodically determine whether it offers or maintains covered accounts. As part of this determination, a financial institution or creditor must conduct a risk assessment to determine whether it offers or maintains covered accounts described in paragraph (b)(3)(ii) of this section, taking into consideration:

(4) The methods it provides to open its accounts;

(5) The methods it provides to access its accounts; and

(6) Its previous experiences with identity theft."

A. **Purpose** – The risk assessment required per 12 CFR Part 41 Subpart J (c) determines if a Bank has covered accounts and, consequently, must develop a formal Identity Theft Prevention Program. The risk assessment must be updated periodically based on changes in methods used to open accounts, methods available to access accounts and the Bank's experience with identity theft.

B. **Risk Factors** - Based on the Bank's Identity Theft Prevention Program Risk Assessment, the following risk factors have been identified:

Types of covered accounts offered:

a. Cash management

b. Credit Accounts

c. Custodian services

d. Deposit Accounts

e. Lending Accounts

f. Safety deposit boxes or other safekeeping services

g. Trust Services

Methods to open a covered account:

- In person

Methods to access a covered account:

- In person

C. **Threats and Risk Levels** - The Identity Theft Risk Assessment follows a qualitative model. Risk levels are determined by considering the likelihood and potential damage of an event as defined below.

Likelihood definitions:

- **Low:** Identity Theft is not expected, but there's a slight possibility it may occur at some time.
- **Medium:** Identity Theft might occur at some time based on a history of limited occurrence, type of covered account, and size and complexity of the bank.
- **High:** Identity Theft will probably occur based on a history of frequent occurrence, type of covered account, and size and complexity of the bank.

Damage Potential definitions:

- **Minimal:** Identity Theft may result in the minor loss of some resources and reputation.
- **Moderate:** Identity Theft may result in loss of resources and reputation which could harm the Bank's ability to achieve its mission.
- **Major:** Identity Theft may result in the loss of major resources and reputation which would harm the Bank's ability to achieve its mission.

Risk Level definitions:

- **Low:** Impact is minimal and could even be considered a cost of doing business.
- **Medium:** Impact could be significant and possibly affect the stability of the Bank.

- **High:** Impact is major and could threaten the stability of the Bank.

V. MISCELLANEOUS IDENTITY THEFT METHODS

General – Social engineering is the attempt to manipulate or fool a person into providing confidential information to an individual that is not authorized to receive such information.

The following subtopics are common types of social engineering with respect to banking.

Pretext Calling – Pretext calling is a fraudulent means of obtaining an individual's personal information. Possessing limited information, such as a customer's name, address and/or social security number, a pretext caller may pose as a customer or an employee in an attempt to convince a Bank employee to divulge confidential information. Information obtained through pretext calling may be sold to debt collection services, attorneys and private investigators for use in court proceedings. Identity thieves may also engage in pretext calling to obtain personal information for use in creating fraudulent accounts. In some instances, pretext callers may call the Bank repeatedly until the caller finds an employee willing to provide the information.

The following demonstrates possible pretext caller situations where extra care should be taken by Bank personnel to ensure the authenticity of the caller:

1. A caller who tries to distract an employee by being overly friendly or engaging in unrelated conversation in an effort to change the employee's focus;

2. A caller who cannot provide all relevant or requested information;

3. A caller who tries to get an employee to circumvent Bank policy through some tactic that is intended to persuade the employee;

4. A caller who is abusive and attempts to get information through intimidation;

5. An employee caller whose caller ID does not agree with that employee's location; or

6. An employee caller that cannot provide basic security information that is readily available to all employees.

Pretext callers may call several times in an effort to obtain bits of information until they build a complete customer profile, and in some situations obtain information about Bank employees.

As such, each branch or department customer contact area should implement specific procedures to protect customer information from being inappropriately released to third parties. Each employee should be responsible for understanding and complying with these procedures.

Dumpster Diving – Dumpster diving is a common method for identity thieves to obtain confidential information that is carelessly thrown away. Dumpster diving involves rummaging through a company's trash to collect customer information, such as office trash cans or large dumpsters.

The Bank has implemented the following procedures to mitigate the risk of dumpster diving:

1. **Shred Bins**: Bank employees are to place any documents that contain confidential company or customer information into designated shred bins located throughout the Bank. Items placed in shred bins are then to be transported to the Bank's designated paper shredders for disposal on a daily basis.

2. **Paper Shredders:** In the event shred bins are not available, Bank employees must utilize individual paper shredders to destroy confidential information.

Shoulder Surfing – Shoulder surfing is used by criminals that acquire personal information through eavesdropping. Shoulder surfers may obtain information while standing in line at a branch or ATM. Others may use binoculars to spy on their victims, while some may stand outside branch windows and observe computer screens that contain confidential account information. In all instances, the objective is to obtain confidential information.

The Bank has implemented the following procedures to mitigate the risk of shoulder surfing:

1. Computer monitors are to be positioned in a manner that prevents individuals from observing confidential information. If this is not feasible then a protective screen is to be utilized on the monitor to prevent others from easily viewing the contents.

2. Ensure that the sharing of confidential information is provided in writing when in a face-to-face situation with a customer. This method prevents someone from learning the information through eavesdropping. This same practice applies when an employee provides a customer with confidential information, and to properly dispose of such information after it has been provided; and

3. Ensure that adequate space exists between customers conducting transactions and other customers standing in line. Proper spacing enhances customer privacy and deters criminals from acquiring confidential information such as PIN, account number, balance, etc.

Card Issuance, Reissuance, and Control Standards - Records of issued cards will be balanced daily to the electronic data processing report total of new and reissued cards. The daily record of issued, spoiled, and on-hand cards at the embossing unit will be reconciled periodically by an independent person. Incoming shipments of cards will be examined for tampering and properly entered into the log of cards received; all of this will be handled via dual control.

Plain envelopes are to be used for mailing cards to customers to reduce the exposure to theft. Follow-up letters are sent to cardholders shortly after the cards are mailed to ascertain that the cards have been received. Control is established over cards returned (either by the customer for cancellation or by the post office as undeliverable) so that:

1. The mail is opened under joint custody.
2. The returned cards are placed under dual control.
3. A single employee should not be in possession of both a PIN and card that has been returned.
4. Cards for which a correct address can be found are re-mailed immediately.
5. Cards for which no address can be found are destroyed.

An expiration date will be printed on each card. An annual fee for reissuance on expiration will be assessed each customer. The card accounts of obligors with previously charged-off balances or otherwise unsatisfactory credit histories with the bank will not be reissued on expiration.

VI. ADMINISTRATION OF THE PROGRAM

A. **Updating the Program** – The Bank will update the Program (including a review of relevant Red Flags) periodically, to reflect changes in risks to customers or to the safety and soundness of Etana from identity theft based on factors such as:

   a. The experiences of the Bank with identity theft.

   b. Changes in methods of identity theft.

   c. Changes in methods to detect, prevent and mitigate identity theft.

   d. Changes in the types of accounts that the Bank offers or maintains.

e. Changes in the business arrangements of the Bank including mergers, acquisitions, alliances, joint ventures and service provider arrangements.

B. **Oversight of the Program** - The responsibility of maintaining an effective Identity Theft Prevention Program is assigned to the Board of Directors. The Board of Directors will be responsible for the appointment of an Identity Theft Prevention Coordinator. The current Identity Theft Prevention Coordinator will be Identity Theft Program Officer. The Identity Theft Prevention Coordinator will report to the Board of Directors.

The Identity Theft Prevention Coordinator will:

a. Work closely with the Bank's senior management and front-line personnel to identify, detect and respond to appropriate Red Flags,

b. Assign specific responsibility for the Program's implementation,

c. Approve material changes to the Program as necessary to address changing identity theft risks, and

d. Report to the Board of Directors at least annually on the compliance of the Program. The report should address material matters related to the Program and evaluate issues such as:

- The effectiveness of the policies and procedures of the Bank in addressing the risk of identity theft in connection with the opening of covered accounts and with respect to existing covered accounts,
- Service provider arrangements,
- Significant incidents involving identity theft and management's response, and
- Recommendations for material changes to the Program.

C. **Oversight of Service Providers** - Whenever the Bank engages a service provider to perform an activity in connection with one or more covered accounts, Etana will take the necessary steps to ensure that the activity of the service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent and mitigate the risk of identity theft.

- ❖ For example, the Bank might require the service provider by contract to have policies and procedures in place to detect relevant Red Flags that may arise in the performance of the service provider's activities, and either report the Red Flags to the Bank or take appropriate steps to prevent or mitigate identity theft.

D. **Staff Training** – The Bank needs to educate employees to identify and respond to Red Flags. Training supports security awareness and strengthens compliance with the Identity Theft Prevention Program. Ultimately, the behavior and priorities of senior management heavily influence the level of employee awareness and policy compliance, so training and the commitment to security starts with senior management. Staff will be trained as necessary to effectively implement the Program. Training materials for the Bank will review the identification, detection and response to Red Flags.

VII. ALERTS, NOTIFICATIONS OR WARNINGS

A. **Consumer Report Address Discrepancy** –

a. Red Flag – A consumer reporting agency provides a notice of address discrepancy.
b. Detection – A consumer report is run for all new loan accounts. Consumer reports are reviewed by a loan officer.
c. Response – Determine from the consumer or customer why the consumer report provided a notice of address discrepancy.
   Confirm the address of the consumer or customer by:
   - Verifying the customer's address with the address the Bank has on file.
   - Verifying the customer's address through a third party.
d. Verification – Review procedures to run consumer reports on a regular basis. Ensure appropriate employees are trained to adequately review consumer reports.
e. Responsibility – Identity Theft Prevention Coordinator.

B. Consumer Report Alert –

a. Red Flag – A fraud or active-duty alert is included with a consumer report.
b. Detection – A consumer report is run for all new loan accounts. Consumer reports are reviewed by a loan officer.
c. Response – Determine from the consumer or customer the reason for the alert.
d. Verification – Review procedures to run consumer reports on a regular basis. Ensure appropriate employees are trained to adequately review consumer reports.
e. Responsibility – Identity Theft Prevention Coordinator

C.**. Consumer Report Credit Freeze** –

a. Red Flag – A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.
b. Detection – A consumer report is run for all new loan accounts. Consumer reports are reviewed by a loan officer.
c. Response – Determine from the consumer or customer the reason for the credit freeze.
d. Verification – Review procedures to run consumer reports on a regular basis. Ensure appropriate employees are trained to adequately review consumer reports.
e. Responsibility – Identity Theft Prevention Coordinator

D. **Consumer Report Unusual Activity Pattern** –

a. Red Flag – A consumer report indicates a pattern of activity inconsistent with the history and usual pattern of activity of an applicant or customer, such as:
   - A recent and significant increase in the volume of inquiries;
   - An unusual number of recently established credit relationships;
   - A material change in the use of credit, especially with respect to recently established credit relationships;
   - An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.
b. Detection – A consumer report is run for all new loan accounts. Consumer reports are reviewed by a loan officer.
c. Response – Determine from the consumer or customer why the consumer report reflects a pattern of unusual activity.
d. Verification – Review procedures to run consumer reports on a regular basis. Ensure appropriate employees are trained to adequately review consumer reports.
e. Responsibility – Identity Theft Prevention Coordinator

E. **Suspicious Documents** –

a. **Application Appears to be Altered or Forged** –

1. Red Flag – An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.
2. Detection – Prior to opening a new account, a consumer or customer is required to complete an application.
3. Response – Determine from the consumer or customer the reason for the appearance of the application. If necessary, require the consumer or customer to resubmit a new application.
4. Verification – Ensure appropriate employees are trained to review applications.
5. Responsibility – Identity Theft Prevention Coordinator

b. **Documents Altered or Forged** –

1. Red Flag – Documents provided for identification appear to have been altered or forged.
2. Detection – Consumer and customer identity is verified prior to opening an account or making changes to an account (i.e., address change). Documents used to verify a customer's identity may include:
   - For an individual – Unexpired, government-issued identification evidencing nationality or residence and bearing a photograph or similar safeguard, such as driver's license or passport.
   - For a person other than an individual (such as a corporation, partnership, or trust) – Documents establishing the existence of the entity, such as certified articles of incorporation, a government-issued business license, a partnership agreement or trust instrument.
3. Response – Determine from the consumer or customer the reason for the appearance of the documents. If necessary, obtain verification of identity from the customer via other means.
4. Verification – Ensure appropriate employees are trained to adequately review documents provided for identification purposes.
5. Responsibility – Identity Theft Prevention Coordinator

c. **Information on ID Inconsistent with Information on File** –

1. Red Flag – Other information on the identification is not consistent with readily accessible information that is on file with the Bank, such as a signature card or a recent check.
2. Detection – Consumer and customer identity is verified prior to opening an account, or making changes to an account (i.e., address change). Documents used to verify a customer's identity may include:
   - For an individual, unexpired government-issued identification evidencing nationality or residence and bearing a photograph or similar safeguard, such as driver's license or passport.
   - For a person other than an individual (such as a corporation, partnership, or trust), documents showing the existence of the entity, such as certified articles of incorporation, a government-issued business license, a partnership agreement, or trust instrument.
3. Response – Determine from the consumer or customer the reason for the inconsistency of their information. If necessary, obtain verification of identity from the customer via other means.
4. Verification – Ensure appropriate employees are trained to adequately review documents provided for identification purposes.
5. Responsibility – Identity Theft Prevention Coordinator

d. **Information on ID Inconsistent with Information Provided** –

1. Red Flag – Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.
2. Detection – Consumer and customer identity is verified prior to opening an account or making changes to an account (i.e., address change). Documents used to verify a customer's identity may include:
   - For an individual - Unexpired, government-issued identification evidencing nationality or residence and bearing a photograph or similar safeguard, such as driver's license or passport.
   - For a person other than an individual (such as a corporation, partnership, or trust) - Documents establishing the existence of the entity, such as certified articles of incorporation, a government-issued business license, a partnership agreement or trust instrument.
3. Determine from the consumer or customer the reason for inconsistency of the information. If necessary, obtain verification of identity from the consumer or customer via other means.
4. Verification – Ensure appropriate employees are trained to adequately review documents provided for identification purposes.
5. Responsibility – Identity Theft Prevention Coordinator.

e. **Photograph or Physical Description Inconsistency** –

1. Red Flag – The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.
2. Detection – Consumer and customer identity is verified prior to opening an account or making changes to an account (i.e., address change). Documents used to verify a customer's identity may include:
   - For an individual - Unexpired, government-issued identification evidencing nationality or residence and bearing a photograph or similar safeguard, such as driver's license or passport.
   - For a person other than an individual (such as a corporation, partnership, or trust) - Documents establishing the existence of the entity, such as certified articles of incorporation, a government-issued business license, a partnership agreement or trust instrument.
3. Response – Determine from the consumer or customer the reason for the difference in photograph or physical description. If necessary, obtain verification of identity from the consumer or customer via other means.
4. Verification – Ensure appropriate employees are trained to adequately review documents provided for identification purposes.
5. Responsibility – Identity Theft Prevention Coordinator.

f. **Suspicion Personal Identifying Information** –

- Address or Telephone Number Flags – Red Flag – The address or telephone number provided is the same as or similar to the account number or telephone number submitted by an unusually large number of other persons opening accounts or other customers.
- Detection – Consumer and customer identity is verified through internal and third-party resources prior to opening an account, or making changes to an account (i.e., address change).
- Response – Determine from the consumer or customer the reason the address or telephone number is the same as one submitted by numerous other accounts. If necessary, obtain verification of identity from the consumer or customer via other means.
- Verification – Ensure appropriate employees are trained to adequately review documents provided for identification purposes.
- Responsibility – Identity Theft Prevention Coordinator.

1. Challenge Question Responses Unavailable or Limited –
   - Red Flag – For banks and creditors that use challenge questions, the person opening the covered account, or the customer cannot provide

authenticating information beyond that which generally would be available from a wallet or consumer report.

- Detection – Customer identity is verified prior to opening an account or making changes to an account (i.e., address change).
- Response – Determine the reason for the inconsistency. If necessary, obtain verification of identity from the customer via other means.
- Verification – Ensure appropriate employees are trained to properly identify a customer.
- Responsibility – Identity Theft Prevention Coordinator.

g. **Incomplete Application** –

1. Red Flag – The person opening the covered account, or the customer fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.
2. Detection – Prior to opening a new account, a consumer or customer is required to complete an application.
3. Response – Review the incomplete parts of the application. Determine from the consumer or customer why the application is incomplete. Require the consumer or customer to complete the required portions of the application.
4. Verification – Ensure appropriate employees are trained to review applications.
5. Responsibility – Identity Theft Prevention Coordinator.

h. **Personal ID Association with Known Fraudulent Activity** -

1. Red Flag – Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the Bank or creditor. For example:
   - The address on an application is the same as the address provided on a fraudulent application;
   - The phone number on an application is the same as the number provided on a fraudulent application.
2. Detection – Consumer and customer identity is verified through internal and third-party resources prior to opening an account or making changes to an account (i.e., address change).
3. Response – Determine from the consumer or customer the reason the personal identifying information is associated with known fraudulent

activity. If necessary, obtain verification of identity from the consumer or customer via other means.

4. Verification – Ensure appropriate employees are trained to adequately review documents provided for identification purposes.
5. Responsibility – Identity Theft Prevention Coordinator.

i. **Personal ID is Inconsistent with External Information** –

1. Red Flag – Personal identifying information provided is inconsistent when compared against external information sources used by the Bank or creditor. For example:
   - The address does not match any address in the consumer report;
   - The Social Security Number (SSN) has not been issued or is listed on the Social Security Administration's Death Master File.
2. Detection – Consumer and customer identity is verified through third party resources prior to opening an account, or making changes to an account (i.e., address change).
3. Response – Determine from the consumer or customer the reason for the inconsistency. If necessary, obtain verification of identity from the consumer or customer via other means.
4. Verification – Ensure appropriate employees are trained to adequately review documents provided for identification purposes.
5. Responsibility – Identity Theft Prevention Coordinator.

j. **Personal ID is Inconsistent with Information on File** –

1. Red Flag – Personal identifying information provided is not consistent with personal identifying information that is on file with the Bank or creditor.
2. Detection – Consumer and customer identity is verified prior to opening an account or making changes to an account (i.e., address change).
3. Response – Determine from the consumer or customer the reason for the inconsistency. If necessary, obtain verification of identity from the consumer or customer via other means.
4. Verification – Ensure appropriate employees are trained to adequately review documents provided for identification purposes.
5. Responsibility – Identity Theft Prevention Coordinator

k. **Personal ID is Inconsistent with Other Personal ID** –

1. Red Flag – Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the

customer. For example, there is a lack of correlation between the SSN range and date of birth.

2. Detection – Consumer and customer identity is verified through internal and third-party resources prior to opening an account, or making changes to an account (i.e., address change). The information is reviewed for discrepancies or inconsistencies.
3. Response – Determine from the consumer or customer the reason for the inconsistency. If necessary, obtain verification of identity from the consumer or customer via other means.
4. Verification – Ensure appropriate employees are trained to adequately review documents provided for identification purposes.
5. Responsibility – Identity Theft Prevention Coordinator.

l. **Personal ID is of a Type Common to Fraudulent Activity** -

1. Red Flag – Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the Bank or creditor. For example:
   - The address on an application is fictitious, a mail drop or a prison;
   - The phone number is invalid or is associated with a pager or answering service.
2. Detection – Consumer and customer identity is verified through internal and third-party resources prior to opening an account or making changes to an account (i.e., address change).
3. Response – Determine from the consumer or customer the reason the information appears to be unusual. If necessary, obtain verification of identity from the consumer or customer via other means.
4. Verification – Ensure appropriate employees are trained to adequately review documents provided for identification purposes.
5. Responsibility – Identity Theft Prevention Coordinator.

I. The SSN has been Submitted by Other Persons –

1. Red Flag – The SSN provided is the same as that submitted by other persons opening an account or other customers.
2. Detection – Consumer and customer identity is verified prior to opening an account, or making changes to an account (i.e., address change).
3. Response – Verify with the customer the SSN they provided is correct.
4. Verification – Ensure appropriate employees are trained to adequately review documents provided for identification purposes.
5. Responsibility – Identity Theft Prevention Coordinator.

F. **Unusual Use or Suspicious Activity** –

a. Account Use is Inconsistent with Normal Activity –

1. Red Flag – A covered account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example:
   - Nonpayment when there is no history of late or missed payments;
   - A material increase in the use of available credit;
   - A material change in purchasing or spending patterns;
   - A material change in electronic fund transfer patterns in connection with a deposit account;
   - A material change in telephone call patterns in connection with a cellular phone account.
2. Detection –The Bank monitors activity on revolving credit accounts for patterns of fraud or inconsistency.
3. Response – Ensure the identity of the customer. Determine from the customer the reason for the unusual pattern.
4. Verification – Ensure appropriate employees are trained to adequately review patterns for covered accounts.
5. Responsibility – Identity Theft Prevention Coordinator.

b. Customer is not Receiving Account Statements –

1. Red Flag – The Bank is notified that the customer is not receiving paper account statements.
2. Detection – The customer notifies the Bank that they are not receiving paper account statements.
3. Response – Ensure the identity of the customer. Ensure the customer is configured to receive paper account statements. Verify the customer's address and, if the address is different from the address on file, determine the reason for the change of address. If a change of address is required, follow appropriate procedures for a change of address.
4. Verification – Ensure appropriate employees are trained to adequately respond to customer requests regarding address changes.
5. Responsibility – Identity Theft Prevention Coordinator

c. **Inactive Account is Used**

1. Red Flag - A covered account that has been inactive for a reasonably lengthy period of time is used (taking into consideration the type of account, the expected pattern of usage and other relevant factors).
2. Detection – Accounts are set to go inactive or dormant after a period of inactivity.
3. Response – Ensure the identity of the customer. Determine from the customer the reason for the account activity.
4. Verification – Ensure appropriate employees are trained to adequately review covered accounts.

5. Responsibility – Identity Theft Prevention Coordinator

d. Key Changes Shortly After Change of Address

1. Red Flag – Shortly following the notice of a change of address for a covered account, the Bank receives a request for a new, additional, or replacement card or a cell phone, or for the addition of authorized users on the account.
2. Detection – The Bank verifies the identity of each customer prior to making key changes such as a request for a new or replacement card or an addition of authorized users on an account.
3. Response – Determine from the customer the reason the changes. Ensure the identity of the customer.
4. Verification – Ensure appropriate employees are trained to identify relevant red flags.
5. Responsibility – Identity Theft Prevention Coordinator.

e. Mail is Returned on an Active Account

1. Red Flag – Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account.
2. Detection – The Bank will attempt to contact the customer with other means (i.e., phone) to determine to reason for returned mail.
3. Response – Ensure the identity of the customer. Determine from the customer the reason mail is being returned.
4. Verification – Ensure appropriate employees are trained to address returned mail.
5. Responsibility – Identity Theft Prevention Coordinator.

f. New Revolving Account Follows Fraud Patterns

1. Red Flag - A new revolving credit account is used in a manner commonly associated with known patterns of fraud patterns. For example:
   - The majority of available credit is used for cash advances or merchandise that is easily convertible to cash (i.e., electronics equipment or jewelry);
   - The customer fails to make the first payment or makes an initial payment but no subsequent payments.
   - Detection – The Bank monitors activity on revolving credit accounts for patterns of fraud or inconsistency.
   - Response – Ensure the identity of the customer. Determine from the customer the reason for the unusual pattern.
   - Verification – Ensure appropriate employees are trained to adequately review patterns for revolving credit accounts.

- Responsibility – Identity Theft Prevention Coordinator.

g. Notification of Unauthorized Changes or Transactions

1. Red Flag – The Bank is notified of unauthorized charges or transactions in connection with a customer's covered account.
2. Detection – The Bank is notified of unauthorized charges or transactions.
3. Response – Have the customer sign an Affidavit of Forgery.
4. Verification – Ensure employees are trained to handle customer notifications regarding unauthorized chargers or transactions.
5. Responsibility – Identity Theft Prevention Coordinator.

G. **Notice Given**

a. Notice that a Fraudulent Account has been Opened

1. Red Flag – The Bank is notified by a customer, a victim of identity theft, a law enforcement authority, or any other person that the Bank has opened a fraudulent account for a person engaged in identity theft.
2. Detection – The Bank is notified a fraudulent account has been opened for a person engaged in identity theft.
3. Response – The Bank will close the account and work with law enforcement.
4. Verification – Ensure employees are trained to respond appropriately to a notification that an account has been opened for a person engaging in identity theft.
5. Responsibility – Identity Theft Prevention Coordinator and have customer complete the attached Identity Theft Affidavit.

H. **Customer Notification of Suspected Identity Theft**

I. **Identity Theft Affidavit**

ETANA CUSTODY

VIII. DEFINITIONS

Act – The Fair Credit Reporting Act.

Account – A continuing relationship established by a person with a financial institution or creditor to obtain a product or service for personal, family, household, or business purposes, including:

- An extension of credit, such as the purchase of property or services involving a deferred payment; and

- A deposit account.

Board of Directors – In the case of a branch or agency of a foreign bank, the managing official in charge of the branch or agency; and

- In the case of any other creditor that does not have a board of directors, a designated employee at the level of senior management.

Covered Account –

- An account that a Bank offers or maintains, primarily for personal, family, or household purposes that involves or is designed to permit multiple payments or transactions such as a credit card account, mortgage loan, automobile loan, margin account, cell phone account, utility account, checking account, or savings account; and

- Any other account that the Bank offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the Bank from identity theft, including financial, operational, compliance, reputation or litigation risks.

Credit – Has the same meaning as 15 U.S.C. 1681 a(r)(5).

Credit – Has the same meaning as in 15 U.S.C. 1681a(r)(5), and includes lenders such as banks, finance companies, automobile dealers, mortgage brokers, utility companies, and telecommunications companies.

Customer – Means a person that has a covered account with a financial institution or creditor.

Financial Institution – A State or National bank, a State or Federal savings and loan association, a mutual savings bank, a State or Federal credit union, or any other person that, directly or indirectly, holds a transaction account belonging to a consumer.

Fraud Alerts

A. **Active-Duty Military Consumer** – A consumer in military service who:

- Is on active duty or is a reservist performing duty under a call or order to active duty under a provision of law; and
- Is assigned to service away from the usual duty station of the consumer.

B. **Fraud Alert, Active-Duty Alert** – A statement in the file of a consumer that:

- Notifies all prospective users of a consumer report relating to the consumer that the consumer may be a victim of fraud, including identity theft, or is an active-duty military consumer, as applicable; and

- Is presented in a manner that facilitates a clear and conspicuous view of the statement by any person requesting such consumer report.

C. **Identity Theft** – A fraud committed using the identifying information of another person, subject to such further definition as the Commission may prescribe, by regulation.

D. **Identify Theft Report** – At a minimum, a report:

- That alleges an identity theft;
- That is a copy of an official, valid report filed by a consumer with an appropriate Federal, State, or local law enforcement agency, including the United States Postal Inspection Service, or such other government agency deemed appropriate by the Commission; and
- The filing of which subjects the person filing the report to criminal penalties relating to the filing of false information if, in fact, the information in the report is false.

E. **New Credit Plan** – A new account under an open-end credit plan (as defined in section 103(i) of the Truth in Lending Act) or a new credit transaction not under an open-end credit plan.

Identity Theft – Has the same meaning as in 12 CFR 1022.3(h).

Red Flag – A pattern, practice, or specific activity that indicates the possible existence of identity theft.

Service Provider – A person that provides a service directly to the financial institution or creditor.

12 CFR Part 41 Subpart J (c) (Periodic Identification of Covered Accounts) states:
"Each financial institution or creditor must periodically determine whether it offers or maintains covered accounts. As part of this determination, a financial institution or creditor must conduct a risk assessment to determine whether it offers or maintains covered accounts described in paragraph (b)(3)(ii) of this section, taking into consideration:

(1) The methods it provides to open its accounts;

(2) The methods it provides to access its accounts; and

(3) Its previous experiences with identity theft."