Identity Theft Protection Policy

|  |  |
| --- | --- |
| Policy Area | IT Policy Library |
| Approved Date | December 31, 20XX |
| Approved By | Policy Committee |
| Effective Date | January 1, 20XX |
| Current Version | 1.0 |

# I. Overview

Policies and procedures help ABC Company meet compliance requirements by addressing identify theft issues in a uniform and consistent manner. For example, they dictate the steps to be followed when we receive a notice of address discrepancy from a consumer reporting agency.

# II. Purpose

The purpose of the Identity Theft Protection Policy is to establish the rules for the creation, monitoring, control, and maintenance of covered accounts.

# III. Scope

This policy applies to all ABC Company Staff that have access to ABC Company’s customer information.

# IV. Policy

A. Program Coordinator

ABC Company has appointed a Program Coordinator of our Identity Theft Red Flags Program. The Program Coordinator shall prepare an identity theft Risk Assessment Report to determine whether ABC Company offers or maintains covered accounts as defined in the Fair and Accurate Credit Transaction Act of 2003 (“FACTA”). At a minimum, the Risk Assessment Report shall review the accounts and services offered, assess past incidents, document suspicious information, evaluate identity theft detection methods, and assess response procedures.

The Program Coordinator shall design, implement, and maintain policies and procedures implementing identity theft detection procedures, response procedures, and an Identify Theft Protection Program to address identity theft and satisfy the requirements of FACTA legislation. The Identity Theft Protection Program shall include, but not be limited to, services offered, policies and procedures related to identity theft, relevant red flags, detection, prevention, and mitigation actions, as well as updates to the Identity Theft Protection Program.

Specific responsibilities that have been delegated to the Program Coordinator include:

* Identifying and assessing the risks of identity theft and discovery of address discrepancies in each relevant area of the Company’s operation, and evaluating the effectiveness of current safeguards that have been implemented to control these risks and to respond to situations in an appropriate fashion.
* Designing and implementing policies and procedures that are appropriate for the size and complexity of our Company and its operations considering the nature and scope of our activities and the sensitivity of the customer information we collect, store, and share with others.
* Regularly monitoring and testing the policies and procedures for compliance with all applicable law and to determine the effectiveness of our procedure in preventing identity theft.
* Assisting with the selection of appropriate service providers that are capable of maintaining safeguards to protect against identity theft and reviewing service provider contracts to ensure that each maintains appropriate procedures for identifying and responding to situations involving identity theft.
* Evaluating and adjusting this procedure in light of relevant circumstances, including changes to ABC Company’s operations, business relationships, technological developments and/or other matters that may impact the security or integrity of customer information and response to identity theft.

The Program Coordinator is the contact person for law enforcement agencies to communicate possible situations of identity theft. Upon receiving a request for information from any law enforcement agency, the Program Coordinator will:

* Provide the law enforcement agency with his/her name, title, and appropriate contact information, such as a mailing address, e-mail address, telephone number and facsimile number, and notify the law enforcement agency promptly of any modifications with respect to contact information.
* If ABC Company has identified possible identity theft or becomes aware of an address discrepancy, the Program Coordinator will send a Report to the customer, as necessary, and to the appropriate law enforcement agency that contains:
  1. The name of the individual, entity or organization
  2. The account numbers or, in the case of transactions, the date and type of each transaction
  3. The Social Security Number, taxpayer identification number, passport number, date of birth, address, or other personal identifying information provided by the individual or entity at the time of the transaction.

To assist in compliance with applicable state and federal regulations, the Program Coordinator will audit the Company’s Policies and Procedures at least bi-annually to determine if the current system is operating effectively to prevent/detect identity theft and to deal with notice of any address discrepancy. Any modification of the system that the Program Coordinator deems appropriate will be implemented as soon as reasonably possible. As part of the audit program, Company personnel will be encouraged to advise the Program Coordinator of any newly identified risks to customers or to the safety of the Company regarding identity theft. To the extent of any newly identified risk that is discovered, the Program Coordinator is authorized to take appropriate action to address the risk, including assessment, independently or through third parties, of the severity of this risk, and make modifications of the audit system by written instruction to all necessary personnel or through obtaining outside products or services to alleviate the risk.

At least annually, the Program Coordinator will report to management:

1. The effectiveness of the Program
2. Explaining “significant events” involving identity theft and management’s response to any incident
3. Providing recommendations for substantive/material changes to the Policies and Procedures due to evolving risks and methods of identity theft.

B. Employee Management and Training

All current employees and new hires, as well as independent contractors who provide services to or that perform services on behalf of ABC Company, will:

* Be subject to satisfactory reference and consumer/criminal report investigations, where appropriate.
* Only have access to customer information if they have a business reason for seeing it.
* Participate in the Company’s privacy policies and information security standards and identity theft and notice of address discrepancy training program and attend education and training seminars on a regular basis, if not otherwise provided for by any independent contractor for its own employees.
* Sign and acknowledge his/her agreement to this procedure.
* Be responsible for protecting the confidentiality and security of the customer information our Company collects and for using the information in accordance with our Policies and Procedures.
* Not be permitted to post passwords near their computers or share passwords with any other person.
* Refer telephone calls or other requests for customer information to the Program Coordinator or appropriate manager when such requests are not received within the ordinary course of the Company’s business or are for information that the employee is not authorized to provide.
* Disclose to service providers, marketers or any other parties only that customer information which is necessary to complete a transaction initiated by the customer and/or as permitted by law. If an employee is unsure as to whether a specific disclosure is permitted, he or she will be instructed to check with the Program Coordinator or appropriate manager prior to releasing the information.
* Be required to notify the Program Coordinator or appropriate manager immediately of any attempts by unauthorized persons to obtain access to customer information and/or if any password or customer information is subject to unauthorized access.

When an employee ceases to be employed by the Company, he/she will be required to turn in any keys in his/her possession that provide access to the Company and file cabinets, desks, and offices in the Company; passwords and security codes, if applicable, will be deleted; and employees will not be permitted to take any customer information from the Company.

C. Obtaining Customer Information and Verifying Customer identities

The following procedures will be implemented with respect to obtaining customer information and verifying customer identities:

* Forms utilized by the Company request customer information, such as names, addresses, telephone numbers, birth dates, social security numbers, tax identification numbers, and driver’s license and insurance information, to enable the Company to verify the identification of its customers. In addition, customers must sign documentation, including sworn statements in some cases, wherein the customer represents and warrants that he/she is the person identified in the documentation.
* Employees will request to see the customer’s driver’s license or other form of government-issued identification bearing a photograph to verify the customer’s identity and will make a copy of the same to retain in the customer’s file. If a customer requests financing in connection with a transaction, the customer will be required to provide employment information and references and must authorize the Company to obtain a credit report, all of which may be utilized to verify the identity of the customer and be used to check for any notice of an address discrepancy. Employees may also request copies of the customer’s utility bills, bank or credit card statements and paycheck stubs.
* In the event that customer information provided is conflicting or cannot be verified upon further inquiry, employees shall request additional government-issued documentation evidencing the customer’s residence and bearing a photograph or other safeguard (i.e. a social security card, alien identification card, or passport) to enable employees to form a reasonable belief that they know a customer’s true identity. When appropriate, employees shall write a summary of the means and results of any measures taken to identify a customer, including the resolution of any discrepancy in the identifying information obtained. Employees will be instructed to notify the Program Coordinator if customer information still cannot be verified, or if the employees have obtained information regarding an address discrepancy that cannot be explained.
* Paper and electronic records containing customer information and relevant to the Company’s identity verification process will be retained by the Company in accordance with federal and state record retention requirements. Upon the expiration of the appropriate retention period, any such records will be disposed of in a secure manner in accordance with the Company’s information security standards.

D. Information Systems

The following information security standards will be implemented in order to protect customer information collected and maintained by our Company:

* Employees will have access only to that customer information which is necessary to complete their designated responsibilities. Employees shall not have access to or be authorized to provide any other unauthorized person access to customer information that is obtained during the course of employment. Requests for customer information that are outside the scope of the Company’s ordinary business or the scope of an employee’s authorization must be directed to the Program Coordinator or designated individuals.
* Access to electronic customer information will be password controlled. Every employee with access to the Company’s computer system and electronic records will have a unique password consisting of at least characters, including numbers and letters. Only employees that need to access electronic records will be provided with authorized access.
* All paper and electronic records will be stored in secure locations to which only authorized employees will have access. Any paper records containing customer information must be stored in a deal jacket or folder. Paper records must be stored in an office, desk, or file cabinet that is locked when unattended. Electronic records will be stored on a secure server that is located in a locked room and is accessible only with a password. Where appropriate, records will be maintained in a fireproof file cabinet and/or at an offsite location. Customers, vendors, and service providers shall not be left in an area with insecure customer records.
* Backups of the computers and/or server will be made at least once every day, or at more frequent intervals as deemed necessary. At least once each month the backup information will be verified. Backup disks will be stored in a locked file cabinet.
* Virus protection software shall be installed on computer systems and new virus updates will be checked at regular intervals. All computer files will be scanned at least once each month, or at more frequent intervals as deemed necessary.
* Firewalls and security patches from software vendors will be downloaded on a regular basis.
* All data will be erased from computers, disks, hard drives, or any other electronic media that contain customer information before disposing of them and, where appropriate, hard drives will be removed and destroyed. Any paper records will be shredded and stored in a secure area for an authorized disposal/recycling service.
* Employees will log off of all Internet, e-mail and other accounts when not being used. Employees will not be permitted to download any software or applications to Company computers or open e-mail attachments from unknown sources. Electronic records may not be downloaded to a disk or individual computer without explicit authorization from the Program Coordinator.
* Electronic records will not be stored online and are not accessible from the internet. If customer information is transmitted electronically over external networks, the information will be encrypted at the time of transmittal.
* Neither current nor former employees will be permitted to remove any customer information from the Company, whether contained in paper records or electronic records, or to disclose our information security standards to any person without authorization from the Program Coordinator.

E. Selection and Oversight of Service Providers

In order to protect the customer information our Company collects, and to deal with alerts and notices, we will take steps to evaluate and oversee our service providers. The following evaluation criteria will be utilized in selecting service providers:

* Compatibility and willingness to comply with the Company’s policies and procedures and the adequacy of the service provider’s own policies and procedures.
* Records to be maintained by the service provider and whether the company will have access to information maintained by the service provider.
* The service provider’s knowledge of regulations that is relevant to the services being provided, including privacy, identity theft, and other consumer protection regulations.
* Experience and ability to provide the necessary services and supporting technology for current and anticipated needs.
* Functionality of any service or system proposed and policies concerning maintaining secure systems, intrusion detection and reporting systems, customer authentication, verification, and authorization, and ability to respond to service disruptions.
* Service and support that will be provided in terms of maintenance, security, and other service levels.
* Financial stability of the service provider and reputation with industry groups, trade associations, and other organizations.
* Contractual obligations and requirements, such as the term of the contract; prices; software support and maintenance; training of employees; customer service; rights to modify existing services performed under the contract; warranty, confidentiality, indemnification, limitation of liability and exit clauses; guidelines for adding new or different services and for contract re-negotiation; compliance with applicable regulatory requirements; records to be maintained by the service provider; notification of material changes to services, systems, controls and new service locations; insurance coverage to be maintained by the service provider; and use of the Company’s data, equipment, and system and application software.
* The right of the Company to audit the service provider’s records, to obtain documentation regarding the resolution of disclosed deficiencies, and to inspect the service provider’s facilities.

Service Providers will be required to agree contractually to be responsible for securing and maintaining the confidentiality of customer information, including agreement to refrain from using or disclosing the Company’s information, except as necessary to or consistent with providing the contracted services, to protect against unauthorized use or disclosure of customer and Company information, to comply with applicable privacy and identify theft regulations, and to fully disclose breaches in security resulting in unauthorized access to information that may materially affect the Company or its customers and to notify the Company to the services provider’s corrective action.

Service Providers will be subject to ongoing assessment to evaluate their consistency with selection criteria, performance and financial conditions, and contract compliance.

F. Identity Theft Detection

The Program Coordinator will implement audit and oversight procedures as he/she deems necessary to detect the improper disclosure or theft of customer information or notices of any address discrepancy and to ensure that employees, independent contractors, and Service Providers are complying with our Company’s Policies and Procedures.

Identity theft detection procedures can include:

* Follow Bank Secrecy Act procedures
* Follow Anti-money Laundering procedures
* Follow Customer Identification Program procedures
* Investigated alerts from Consumer Reporting Agency (CRA)
* Inspect application documents
* Inspect identification documents
* Compare identification information to internal information for other similar account holders
* Verify that identification document presented is of the type issued by a government
* For online applications, confirm that IP address is consistent with the applicant’s indicated geographic location
* Validate Social Security Number
* Use shared secrets (e.g., the applicant is asked for information only the institution and the applicant knows)
* Review county of residence
* Require multiple confirmations of true identity
* Use of external databases (CRA, public records)
* Procedures exist for changes to account information such as postal address
* On-line access to accounts is locked after a number of invalid sign in attempts, written reactivation procedure exists

G. Identity Theft Response Procedures

In the event of a breach, or at any other time as the Program Coordinator deems appropriate, the Program Coordinator may modify or supplement our Company’s Policies and Procedures.

If the Company experiences an identity theft breach, the Program Coordinator will inform management and will take appropriate steps to notify counsel, Service Providers, customers, and the appropriate law enforcement agency of any breach, damage or loss of information and the risks associated with the same and will immediately take measures to limit the effect of the breach, identify the reason for the breach and implement procedures to prevent further breaches.

Identity theft response procedures can include:

* Determine whether a suspicious activity report (SAR) should be filed
* When identify theft is detected in an account, investigate the account holder’s other accounts for identity theft
* For online account access, if an IP address is not recognized, require the account holder to answer a challenge question
* In the event of failed website or automated telephone authentication, require applicant or account holder to contact a service representative
* When to investigate Red Flag and temporarily suspend account
* When to investigate Red Flag, but do not suspend account
* Monitor the account for evidence of identity theft
* When to contact the applicant or account holder
* Change passwords, security codes, or other security devices that permit access to a covered account
* Reopen the account with a new account number
* When to refuse to open an account
* When to close existing account

# V. Enforcement

Any Staff member found to have violated this policy may be subject to disciplinary action, up to and including termination.

# VI. Distribution

This policy is to be distributed to all ABC Company Staff who use Information Resources.

**Policy History**

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Description | Approved By |
| 1.0 | 1/1/20XX | Initial policy release |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**References:**

COBIT EDM01.01, APO12.02, APO12.07, APO13.07, DSS03.02, DSS05.02, MEA03.01

GDPR Article 25, 30, 32

HIPAA 164.308(a)(2), 164.308(a)(3)(ii)(B), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(D)

ISO 27001:2013 A.5, A.7.2.2, A.8.1.3, A.8.2.1, A.9-14, A.16-18

NIST SP 800-37 3.4, 3.7

NIST SP 800-53 All XX-1 controls, AC-2, AT-2, AT-3, CP-3, IA-2, IA-8, PL-4, PM-13, PM-29

NIST Cybersecurity Framework ID.AM-5, ID.GV-3, ID.RA-6, PR.AC-1, PR.AT-1, DE.DP-2

PCI 3.7, 4.1, 4.3, 5.1-4, 6.1-2, 6.4, 7.1-3, 8.1-2, 8.4-5, 8.8