2. IDENTITY THEFT PREVENTION PROCEDURES AND GUIDELINES

2.1 Preventing Identity Theft

Security Safeguards

The Company will take reasonable steps to maintain the security and confidentiality of customer information from the point of data entry to the point of data disposal.

- It is the policy of the Company not to use, disclose or permit access to any sensitive personal information of customers except (i) as necessary to initiate, render, bill and collect for services, (ii) as requested and authorized by the customer or (iii) as otherwise permitted or required by law.
- The Company will train employees to be alert to Red Flags and other risks of identity theft in accordance with this Compliance Program and will pass along to its employees information and instructions regarding any new security risks or possible security breaches.
- The Company will implement appropriate access controls for its premises and areas where sensitive customer information is stored.
- When possible, the Company will limit its collection of sensitive personal information to customer information for which the Company has a legitimate business need.
- The Company will keep a customer's sensitive personal information only as long as is necessary in connection with the Company's legitimate business needs.
- Physical and electronic access to customer personal information will be limited to employees who have a business reason to access such information.
- The Company will use password-activated screen savers to lock employee computers after a period of inactivity.
- Customer information will be stored in a room or file cabinet that is locked when unattended.
- Where appropriate and feasible, the Company will avoid storing sensitive customer information on a computer with an Internet connection.
- When customer information is stored on a server or other computer, the Company will ensure that the computer is accessible only by authorized employees using a strong password, and that the computer is kept in a physically secure area.
- Where appropriate and feasible, the Company will maintain secure backup records and keep archived data secure by storing it off-line and in a physically secure area.
- Where appropriate and feasible, the Company will ensure that data storage areas are protected against destruction or damage from physical hazards like fire or floods.
- The Compliance Manager will maintain an inventory of the Company's computers and other equipment on which customer information is stored.
- If the Company must transmit sensitive customer information via e-mail or public networks, the data will be encrypted.
- Where appropriate and feasible, the Company will maintain up-to-date programs and controls to prevent unauthorized access to the Company's network and systems where customer information is stored, including the use of firewalls and intrusion detection systems to prevent security breaches or alert the Company to attempted attacks, and the use of automatic methods of secure

data transmission in any instance where the Company collects customer information online directly from customers.

- Customer information will be disposed of in an appropriate and secure way, including the destruction of physical and electronic records by shredding or pulverizing physical records so that the information cannot be read or reconstructed and by destroying or erasing data when disposing of computers, disks, CDs, magnetic tapes, hard drives, lap tops, PDAs, cell phones or other electronic media or hardware containing customer information.
- The Company will select service providers that can maintain appropriate safeguards and, to the extent appropriate and feasible, will oversee service provider handling of customer information.

System Security Reviews and Evaluation

In addition to implementing the security safeguards listed above, the Compliance Manager will from time to time evaluate (or engage consultants or other third parties to evaluate) the Company's network, policies, procedures and physical security to determine potential security vulnerabilities. The Compliance Manager may evaluate and adjust the Compliance Program from time to time as necessary in light of relevant circumstances, including changes in the Company's business operations or as the result of security testing and monitoring. If the Company has developed such a plan, or in the event that the Compliance Manager determines that development of such a plan is appropriate and feasible, the Compliance Manager may develop and implement a written system and/or data security plan for the Company, which plan will be attached to this Compliance Program as **Annex A** and will be incorporated into this Compliance Program.

Customer Verification and Authentication

The Company will take appropriate steps to obtain identifying information about, and to verify the identity of, any person opening a new covered account or requesting access to an existing covered account. With limited exceptions, the Company will not to use, disclose or permit access to any sensitive personal information of customers except as requested and authorized by the customer. Responsible Employees should take appropriate steps to authenticate customers, monitor transactions and verify change of address and other account change requests for existing covered accounts.

- The Company will take reasonable measures to ensure the validity of customer and third party requests for customer or account information and to validate and confirm customer-authorized disclosures of customer or account information. Customer and account information will be shared based on a customer or third party request only with (i) the customer, (ii) an authorized account user established in accordance with the CPNI Compliance Program, or (iii) a third party for which a customer or authorized account user has expressly requested and authorized the disclosure as required by the CPNI Compliance Program (for requests involving CPNI) or by written authorization and/or confirmation call to the telephone number of record (for requests not involving CPNI). Any time customer information or account information is shared with a third party at the request of the customer or an authorized account user, the Company will notify the customer of the disclosure by notification sent to the customer's address of record. A sample form of customer notification for customer-authorized disclosures is included on **Annex D**.
- For new covered accounts opened in person, a Responsible Employee will request common forms of identification or identifying information in order to verify the identity of the person opening a covered account. The identification of the person opening a covered account may be verified by:
    - requesting a valid photo ID;

- personal knowledge of a Responsible Employee; or
- another reasonable method of verification approved by the Compliance Manager.

- For existing covered accounts, any requests for customer information involving CPNI require customer identification and authentication in accordance with the CPNI Compliance Program, using personal identification with a valid photo ID, passwords, security questions and/or use of the customer's address or phone number of record as required by the CPNI Compliance Program. Requests for customer information not involving CPNI will be verified and customer's authenticated either by (i) using the same methods required by the CPNI Compliance Program, (ii) personal knowledge of a Responsible Employee or (iii) by contacting the customer or an authorized account user at the telephone number of record for confirmation.
- For covered accounts not opened in person (such as accounts opened via telephone or online) the Company will actively monitor account transactions for suspicious activity. Once such accounts have been opened, the account will be considered an existing covered account, and customer identification and authentication procedures shall be the same as listed in the preceding bullet point for existing covered accounts.
- The Company will document all requests made by customers and/or third parties for any customer or account information that includes sensitive personal information or CPNI.
- Any time customer information or account information is shared with a third party at the request and authorization of the customer or an authorized account user, the Company will notify the customer of the disclosure using the customer's address of record in accordance with the CPNI Compliance Program (for requests involving CPNI) or by written notification or confirmation to the telephone number of record (for requests not involving CPNI). A sample form of customer notification for customer-authorized disclosures is included on **Annex D**.
- Changes of address or change of passwords or other account information for all covered accounts will be verified by sending an account change notice to the customer's address of record or by telephone call or voicemail to the telephone number of record. A sample form of customer notification for customer account changes is included on **Annex D**.

2.2 Detecting Red Flags.

The Company has incorporated and may incorporate from time to time into this Compliance Program relevant Red Flags from the following sources: (i) incidents of identity theft that the Company has experienced; (ii) methods of identity theft that the Company has identified that reflect changes in identity theft risks; and (iii) applicable regulatory or law enforcement requirements and guidance, including illustrative examples provided by state and federal agencies or law enforcement authorities. While the specific examples included in this Section are important factors to be considered in every case by Responsible Employees in connection with covered accounts, all employees and representatives of the Company must constantly be alert to circumstances which could indicate identity theft activity. Relevent patterns, practices and specific activities that indicate the possible existence of identity theft include, but are not limited to, the following Red Flags:

- A fraud or active duty alert is included with a consumer report.
- A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.
- A consumer reporting agency provides a notice of address discrepancy.
- A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or customer, such as: (a) a recent and significant increase in the

volume of inquiries; (b) an unusual number of recently established credit relationships; (c) a material change in the use of credit, especially with respect to recently established credit relationships; or (d) an account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

- Documents provided for identification appear to have been altered or forged.
- The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.
- Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.
- Other information on the identification is not consistent with readily accessible information that is on file with the Company, such as a signature card or a recent check.
- An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.
- Personal identifying information provided is inconsistent when compared against external information sources used by the Company. For example: (a) the address does not match any address in the consumer report; or (b) the Social Security Number (SSN) has not be issued, or is listed on the Social Security Administration's Death Master File.
- Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer.
- Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the Company. For example: (a) the address on an application is the same as the address provided on a fraudulent application; or (b) the phone number on an application is the same as the number provided on a fraudulent application.
- Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the Company. For example: (a) the address on an application is fictitious, a mail drop, or a prison; or (b) the phone number is invalid, or is associated with a pager or answering service.
- The SSN provided is the same at that submitted by other persons opening an account or other customers.
- 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.
- 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.
- Personal identifying information provided is not consistent with personal identifying information that is on file with the Company.
- For accounts where the Company uses 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.
- Shortly following the notice of a change of address for a covered account, the Company receives a request for a new, additional, or replacement card or a cell phone, or for the addition of authorized users on the account.

- A new covered account is used in a manner commonly associated with known patterns of fraud patterns. For example, the customer fails to make the first payment or makes an initial payment but no subsequent payments.
- A covered account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example: (a) nonpayment when there is no history of late or missed payments, or (b) a material change in calling or usage patterns in connection with a covered account.
- Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account.
- The Company is notified that the customer is not receiving paper account statements.
- The Company is notified of unauthorized charges or transactions in connection with a customer's covered account.
- The Company is notified by a customer, a victim of identity theft, a law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft.
- Evidence of a compromise of physical or electronic security systems, such as evidence of a break in, hacking of the Company's computer network or systems, or missing documents or electronic storage media.
- Any activity indicative of pretexting or of a CPNI breach.

In the course of their day-to-day activities, Responsible Employees will monitor account activity and transactions related to covered accounts in order to detect and document Red Flags. Responsible Employees encountering any of these situations should report them immediately to the Compliance Manager. Responsible Employees should document the Red Flags in the CSS process described below.

2.3 Documenting Red Flags

This Compliance Program is designed to detect, prevent and mitigate identity theft in connection with the opening of a covered account or any existing covered account. The emphasis of the Compliance Program is to identify risks of identity theft. The Red Flags identified in Section 2.2 are the centerpiece of the Company's identity theft prevention efforts. The CSS is designed to prompt Responsible Employees to be attentive to Red Flags and to develop and record the most useful information for identifying patterns, practices or specific activities that indicate the possible existence of identity theft.

Any potential Red Flags raised in connection with a covered account must be noted on a CSS and brought to the attention of the Compliance Manager, who will then advise the Responsible Employee on an appropriate course of action, which may include further inquiry or investigation. A blank CSS is attached to this Compliance Program as **Annex B**. Responsible Employees must prepare a Compliance Summary Sheet ("**CSS**") whenever a Red Flag is raised in connection with a covered account. The Compliance Manager is responsible for coordinating any Company response based on a completed CSS. The Compliance Manager is also responsible for administering and maintaining any documentation associated with a completed CSS.

Each completed CSS should be forwarded to the Compliance Manager, who will determine whether the CSS is adequately supported with documentation. If it is not, the Compliance Manager will coordinate with the Responsible Employee(s) to obtain a fuller documentary record. It is the responsibility of the Responsible Employee(s) who completed the CSS to update the form as necessary should circumstances materially change over the course of the Compliance Manager's investigation. Based on a complete,

adequately supported CSS, the Compliance Manager will determine an appropriate Company response in accordance with this Compliance Program.

2.4 Responding to Red Flags

It is the policy of the Company to respond appropriately to any Red Flags that are detected in connection with the opening of a covered account or any existing covered account, commensurate with the sensitivity of the information involved and the degree of risk posed.

Upon receiving a complete, adequately supported CSS, the Compliance Manager will conduct an appropriate investigation of the Red Flag and may consult with outside legal counsel and relevant state, federal or local law enforcement authorities. In determining and formulating an appropriate Company response, the Compliance Manager should consider aggravating factors that may heighten the risk of identity theft, such as a data security incident that results in unauthorized access to covered account records held by the Company, or notice that a customer has provided information related to a covered account to someone fraudulently claiming to represent the Company or to a fraudulent website. Appropriate Company responses for Red Flags may include, but are not limited to, one or more of the following:

- monitoring a covered account for evidence of identity theft;
- contacting or notifying the customer, including mandatory customer notification if a Red Flag involves a breach of security or other unauthorized use or access to a customer's sensitive personal information that has resulted or is likely to result in identity theft or financial harm;
- changing any passwords, security codes or other security devices that permit access to a covered account;
- reopening a covered account with a new account number;
- not opening a new covered account;
- closing an existing covered account;
- not attempting to collect on a covered account or not selling a covered account to a debt collector;
- notifying local, state or federal law enforcement authorities, including mandatory law enforcement notification if a Red Flag involves a breach of security or other unauthorized use or access to a customer's sensitive personal information that has resulted or is likely to result in identity theft or financial harm;
- for any Red Flag involving pretexting or a CPNI breach, responding as required by the Company's CPNI Compliance Program; and/or
- determining that no response is warranted under the particular circumstances.

The Company's response to a Red Flag must be documented in writing on the CSS. The documentation must include whether or not the Company decided to contact or notify the customer or law enforcement authorities and the reasons supporting that determination.

In the event of a security breach, the Company will take appropriate steps to preserve the confidentiality and integrity of customer information. Appropriate Company responses for security breaches may include, but are not limited to, one or more of the following:

- taking immediate action to secure any information that has or may have been compromised (for example, if a computer connected to the Internet is compromised, disconnect the computer from the Internet);
- preserving and reviewing files or programs that may reveal how the breach occurred;
- if feasible and appropriate, involving security professionals or consultants as soon as possible to help assess the breach;
- contacting or notifying the customer, including mandatory customer notification if the breach involves unauthorized use or access to a customer's sensitive personal information that has resulted or is likely to result in identity theft or financial harm;
- notifying local, state or federal law enforcement authorities, including mandatory notification to law enforcement if the breach may involve criminal activity or if the breach involves sensitive personal information and there is evidence that the breach has resulted or is likely to result in identity theft or financial harm; and/or
- notifying credit bureaus and/or other businesses that may be affected by the breach, including mandatory notification to other businesses if the breach involves account information for a credit card account, bank account or other account maintained by another business.

Notifying Individuals

In deciding whether notification to individuals is warranted, the Compliance Manager should consider the nature of the Red Flag or security breach, the type of information compromised, the likelihood of misuse, and the potential for identity theft or financial harm. Individuals must be notified if the Red Flag or security breach involves unauthorized use or access to a customer's sensitive personal information (such as Social Security number or credit card or bank account numbers) that results in a reasonable likelihood of identity theft or financial harm. When notifying individuals, the Compliance Manager will:

- consult with outside legal counsel regarding the form of notice to be sent to individuals;
- consult with law enforcement agencies about the timing of the notification to ensure that it does not impede any ongoing investigation; and
- consider using letters, websites and toll-free numbers as methods of communication with those customers whose information may have been compromised.

A sample form of customer notification for security breaches involving sensitive personal information is included on **Annex D**.

Notifying Law Enforcement

When a Red Flag or security breach involves criminal activity or if there is evidence that the breach has resulted or is likely to result in identity theft or financial harm, the Compliance Manager will contact local law enforcement immediately to report the situation and the potential risk for identity theft. If local law enforcement agencies are not familiar with investigating information compromises, the Compliance Manager will contact the local office of the FBI or the U.S. Secret Service using the contact numbers listed in the directory government listings. For any incidents involving mail theft, the Compliance Manager will contact the U.S. Postal Inspection Service using the contact number listed in the directory government listings. For Red Flags or security breaches involving pretexting or a CPNI breach, the Compliance Manager will contact the FBI and U.S. Secret Service using the Federal Communications Commission's central reporting facility in accordance with the CPNI Compliance Program.

Notifying Other Businesses

If customer information such as credit card or bank account numbers is stolen from the Company, the Company will take immediate action to notify the institution which maintains the account so that it can monitor the account for fraudulent activity. If names and Social Security numbers have been stolen, the Compliance Manager may elect to contact the major credit bureaus via telephone or e-mail for additional information or advice:

Equifax
U.S. Customer Services
Equifax Information Services, LLC
Phone: 1-800-685-1111
E-mail: businessrecordsecurity@equifax.com

Experian
Experian Security Assistance
E-mail: BusinessRecordsVictimAssistance@experian.com

TransUnion
Phone: 1-800-372-8391

If the security breach involves a large group of customers, the Compliance Manager should advise the credit bureaus if the Company is recommending that people request fraud alerts for their files.

2.5 Updating the Compliance Program

The Company will update this Compliance Program (including a review and update of relevant Red Flags) on a periodic basis to reflect changes in risks to customers or to the safety and soundness of the Company from identity theft, based on the following factors:

- the experiences of the Company with identity theft;
- changes in methods of identity theft;
- changes in methods to detect, prevent and mitigate identity theft;
- changes in the types of accounts that the Company offers or maintains; and
- changes in the business arrangements of the Company, including mergers, acquisitions, alliances, joint ventures and service provider arrangements.

The Compliance Manager may make changes to this Compliance Program as often as necessary to address changing identity theft risks. Any changes will be included in the Compliance Manager's annual report to the Board of Directors for approval by the Board of Directors at that time.

3. ADMINISTERING THE PROGRAM

3.1 Employee Training

Company staff will be trained, as necessary, to effectively implement this Compliance Program. All Responsible Employees will receive training in the policies and procedures included in this Compliance

Program, both at the initiation of their employment and from time to time thereafter as appropriate, including, for current employees, at the inception of this Compliance Program.

- The Compliance Manager will regularly remind all employees (including but not limited to Responsible Employees) that it is the Company's policy – and a legal requirement – to keep customer personal information and CPNI secure and confidential.
- Every Responsible Employee will be asked to review this Compliance Program upon implementation (for existing Responsible Employees) upon hiring (for new Responsible Employees) and annually thereafter (for all Responsible Employees) and to sign an Employee Statement of Compliance in the form attached to this Compliance Program as **Annex C**.
- Company employees will be trained to take steps to maintain the security, confidentiality and integrity of customer information and CPNI, including:
    - locking rooms and file cabinets where customer records are kept;
    - not sharing or openly posting employee or Company passwords in work areas;
    - not leaving sensitive papers out on their desks when they are away from their workstations;
    - putting files away, logging off of their computers and locking their file cabinets and office doors at the end of the day;
    - not transmitting sensitive customer information electronically via e-mail or public networks unless such data is encrypted;
    - promptly passing along information regarding any new security risks or possible security breaches;
    - being suspicious of pretexting and phone phishing by unknown or unverified callers claiming to need account numbers, CPNI or other customer or account information;
    - referring calls or other requests for customer personal information or CPNI to designated individuals who have been trained in how the Company safeguards such information; and
    - reporting Red Flags and/or actual or potential CPNI breaches to the Compliance Manager immediately.
- Terminated employees will be prevented from accessing customer information by immediately deactivating their passwords and user names and taking other appropriate measures.
- Employees will be subject to discipline, up to and including termination, for failure to comply with this Compliance Program and/or the CPNI Compliance Program.

Once per year, each Responsible Employee must complete the Employee Statement of Compliance attached as **Annex C**. The Compliance Manager will maintain a permanent file of completed employee statements and will address as appropriate any compliance issues identified on any of the completed employee statements.

NO EMPLOYEE WILL BE RETALIATED AGAINST IN EMPLOYMENT FOR FOLLOWING THE POLICIES AND PROCEDURES REQUIRED BY THIS COMPLIANCE PROGRAM, REPORTING ANY BREACH OF SUCH POLICIES AND PROCEDURES, OR PARTICIPATING IN ANY INVESTIGATION RELATING TO A BREACH OF SUCH POLICIES AND PROCEDURES. IF YOU BELIEVE YOU HAVE EXPERIENCED RETALIATION, PLEASE REPORT SUCH ACTION TO THE COMPLIANCE MANAGER,

ANOTHER MEMBER OF SENIOR MANAGEMENT OR THE COMPANY'S LEGAL COUNSEL IMMEDIATELY.

3.2 Recordkeeping

The Compliance Manager will maintain a file for each original CSS and its supporting documentation and will retain all such records for not less than five (5) years.

3.3 Reporting

The Compliance Manager will report to the Board of Directors on an annual basis. The report should address material matters relating to this Compliance Program, including the following:

- the effectiveness of the Company's policies and procedures 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 the Company's response; and
- any material changes made or recommended to be made to the Compliance Program to address changing identity theft risks

3.4 Oversight of Service Provider Arrangements

Whenever the Company engages a service provider to perform an activity in connection with one or more covered accounts, the Company will take steps to ensure that the activities of the service provider are conducted in accordance with reasonable policies and procedures designed to detect, prevent and mitigate the risk of identity theft. When appropriate and feasible, the Company will require such service providers to agree to contractual language or to certify in writing that the service provider has policies and procedures in place to detect, prevent and mitigate patterns, practices or specific activities that indicate the possible existence of identity theft which may arise in the performance of the service provider's responsibilities, and to either report such matters to the Company or otherwise take appropriate steps to prevent or mitigate identity theft. A sample form of service provider certification of identity theft prevention policies and procedures is included on **Annex D**.

4. DEFINED TERMS

Certain capitalized terms used in this Compliance Program are defined where first used herein. Certain other capitalized or uncapitalized terms used in this Compliance Program are, unless the context or circumstances otherwise require, defined as follows:

"**account information**" means information that is specifically connected to the customer's service relationship with the Company, including such things as an account number or any component thereof, the telephone number associated with the account, or the amount of any account billing.

"**address of record**" means a postal or electronic address that the carrier has associated with the customer's account for at least thirty (30) days.

"**covered account**" means (i) an account that the Company offers or maintains primarily for personal, family or household purposes, that involves or is designed to permit multiple deferred payments

for the Company's services, such as residential wireline and wireless telephone accounts, residential cable or digital video accounts, residential DSL or other internet accounts, residential calling card accounts, etc. or (ii) any other account that the Company offers or maintains for which there is a reasonably foreseeable risk to customers or the safety and soundness of the Company from identity theft, including financial, operational, compliance, reputation or litigation risks.

"**CPNI**" means customer proprietary network information, including call detail information and personally identifiable account information subject to the Company's CPNI Compliance Program.

"**CPNI breach**" means any situation when a person, without authorization or exceeding authorization, has intentionally gained access to, used or disclosed CPNI.

"**CPNI Compliance Program**" means the Company's written policies and procedures for the detection and mitigation of pretexting and the prevention of CPNI breaches.

"**customer**" means a person who has a covered account with the Company.

"**identity theft**" means any fraud, including but not limited to pretexting, committed or attempted using the identifying information of another person without authority.

"**telephone number of record**" means the telephone number associated with the underlying service (for any account involving telecommunications service and CPNI) or the telephone number associated with the customer's account (for any account involving services other than telecommunications service).

"**pretexting**" means a form of identity theft where a person uses the identity of another person to gain unauthorized access to the CPNI of that person.

"**Red Flag**" means a pattern, practice or specific activity that indicates the possible existence of identity theft and which has been included in this Compliance Program.

"**sensitive personal information**" means an individual's first name and or first initial and last name *in combination with* any one or more of the following data elements that relates to the individual if any of the data elements are not encrypted, redacted, or otherwise altered by any method or technology in such manner that the name or data elements are unreadable: (i) social security number; (ii) driver's license number or other unique identification number created or collected by a government body; (iii) financial account number, credit card number or debit card number in combination with any required security code, access code, or password that would permit access to the individual's financial account; (iv) unique electronic identifier or routing code, in combination with any required security code, access code or password that would permit access to an individual's financial account; or (v) unique biometric data, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data. For purposes of this Compliance Program "personal information" does not include information that is lawfully obtained from publicly available sources, or from federal, state or local government records lawfully made available to the general public.

"**service provider**" means a person that provides service directly to the Company.

"**valid photo ID**" means a government-issued means of personal identification with a photograph, such as a driver's license, passport or comparable ID that is not expired.