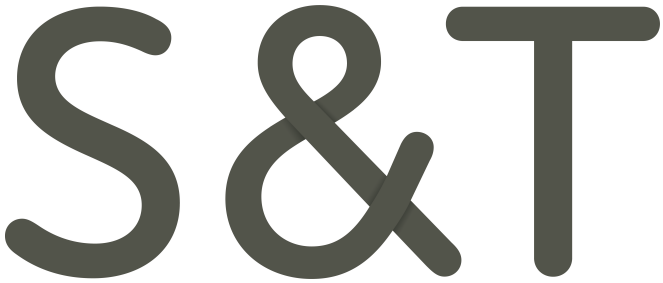
CONSUMER PROTECTION POLICY AND PROCEDURES (IDENTITY THEFT PROGRAM)

OPERATING POLICY AND PROCEDURES

FOR



Approved by: S&T Board of Directors

Date: 3/26/2009

TABLE OF CONTENTS

Policy Statement: Identity Theft Prevention Program Policy

Identity theft is fraud committed or attempted by using the identifying information of another person without his or her authority. Identifying information may include such things as, Social Security number, account number, date of birth, driver's license number, passport number, biometric data and other unique electronic identification numbers or codes. This policy statement serves to communicate to employees what S&T's expectations are to detect, prevent and mitigate the effects of identity theft in order to protect consumers and help ensure safe and sound operations.

Under federal law, S&T, (the "Company") inclusive of its affiliates, has the statutory responsibility to protect the confidentiality of its customers' identity information. This responsibility extends to each and every employee of the Company, including the staff of any affiliates. It is up to all of employees of the Company to guard against the improper or fraudulent disclosure of any customer's confidential and identity information.

The Company complies with specific rules issued by the Federal Communications Commission, such as Customer Proprietary Network Information (CPNI). The Company's Customers' identity information and CPNI could be valuable to other entities and, as such, attempts may be made to get S&T employees to unwittingly disclose this information. If anyone approaches you regarding customers' identity information and/or CPNI, please contact the Compliance Officer immediately.

Compliance Officer
Donita Baird 785-694-2256

If, due to your employment at S&T, you obtain access to a customer's identity information, as well as CPNI, you should treat such information as confidential. When you no longer need a customer's identity information or CPNI, you shall destroy it as described herein.

S&T reserves the right to take disciplinary action, up to termination, for infractions of maintaining confidentially of identity information and/or CPNI rules or for other misconduct. S&T reserves the right to depart from past disciplinary practices at its sole discretion, when it seems such departure desirable and appropriate.

S&T takes seriously its compliance with the federal rules. As part of this endeavor S&T has implemented a system to clearly establish the status of a customer's identifying information and CPNI, and train its personnel as to when they are, and are not authorized to use CPNI.

If you have any questions about CPNI or your role in protecting the privacy of S&T's customers, please contact the Compliance Officer at any time. S&T thanks you for helping protect the privacy of all of our customers.

DEFINTIONS:

Covered Accounts: A covered account is a consumer account designed to permit multiple payments or transactions, or any other account for which there is a reasonable foreseeable risk from identity theft**.**

Creditor: A creditor is any person who regularly extends, renews, or continues credit; any person who regularly arranges for the extension, renewal or continuation of credit; or any assignee of an original creditor who participates in the decision to extend, renew, or continue credit. Creditors include: finance companies, automobile companies, mortgage brokers, utility companies and **telecommunications companies.**

CPNI – Customer Proprietary Network Information
Section 222(h)(1) of the 1996 Telecommunications Act defines CPNI as:

A. Information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and
B. Information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier.

Practically speaking, CPNI includes information such as the phone numbers called by a consumer; the frequency, duration, and timing of such calls; and any services purchased by the consumer, such as call waiting.

Identifying Information: Any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including any:

- Name, SSN, Date of Birth, official state or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number
- Unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation
- Unique electronic identification number, address, or routing code or
- Telecommunications identifying information or access device

Identity Theft: Is a fraud committed or attempted using the identifying information of another person without authority.

Red Flags: A pattern, practice, or specific activity that indicates the possible risk of identity theft.

Service Provider: Any person or entity that provides a service directly to the financial institution or creditor (Company); for example, billing vendors, consultants, and/or collection agents.

I. Identification of Red Flags: This section addresses examples of factors to consider when determining which Red Flags are relevant.

A. The following examples are not all inclusive; therefore as new factors are made known the Compliance Officer or senior management designee will make periodic reviews and note incidents of identity theft in order to update the program accordingly.

1. Types of covered accounts offered and/or maintained. The Company will consider that all accounts will be considered "covered accounts".

2. Methods provided to open accounts.

a) Current CPNI procedures will be adhered to with the following additions:

(a) At retail locations one piece of identification will be required, which must be a government issued photo ID such as, driver's license, passport or other comparable ID that has not expired.

(i) The document should be viewed with a critical eye, looking for any potential forgery, discrepancy in address, manipulation of the document itself, etc.

(ii) Should employee suspect potential identity theft they should immediately contact the Compliance Officer.

(b) Accounts opened via US Mail or fax will require the customer to provide identifying information by one of the following options: 1) have the application form notarized by a certified notary, 2) send a photocopy of two forms of ID (one must be a government issued photo ID and the other must have a name and signature) or the customer may come into the retail location, whereby those procedures, found above at I.A.2.a)(a), will be followed.

3. Methods to limit access to accounts and ensure data security.

a) Only employees that have direct contact with the customer will have immediate access to customer records, such as Customer Service Representatives, supervisors/managers, and accounting as it pertains to customer billing.

b) Employees will have their own log-on identification by which to access the system. The employee log-on information must be kept secure and not shared with others. Computer settings will include the access to be automatically locked after 10 minutes of inactivity.

c) Company lap top computers must be kept secure by protecting them from unauthorized users, as well as installing security measures to access customer identifying information stored on the device or access to the company network.

d) Employees that use paper copies of accounts will be required to lock documents in a file cabinet or their desk when not in use. (Examples: applications, service orders, troubles, credit card receipts, payment receipts, billing records, billing stubs, customer bills, etc)

(a) When an employee transports service orders and troubles for accounts to the jobsite, the employee will keep the copies secured in the company vehicle until returned to the office.

(b) When work with a paper record copy is complete and not necessary for other work, the paper copy will be destroyed, via a paper shredder.

e) Employees who have possession of company or customer computers, for the purpose of troubleshooting and repair, will keep the hardware and backups in a secure/locked location when not in use.

(a) When retiring computer hardware/appliances, the employee will verify that all identifying information is completely destroyed prior to disposal of the hardware or source with identifying information.

f) The S&T IT Manager will maintain the security of customer identifying information and CPNI stored on company servers by limiting access to authorized employees, as determined by the Chief Executive Officer.

(a) Any unauthorized access will be reported to the Compliance Officer immediately.

g) The S&T Chief Financial Officer will protect the security of customer identifying information and CPNI within the company databases by authorizing employee access to the Accounting Master and Customer Master databases, and will monitor additions and changes on a quarterly basis.

(a) Unauthorized additions/changes will be reported to the Compliance Officer immediately.

II. Detection of Red Flags: the detection of any Red Flag is the responsibility of all employees in the Company.

A. Detection of red flags in opening an account will require employees to obtain identifying information about the customer and the verification of the person opening an account.

1. Information will be via a written application, whereby the employee will verify via physical documentation as noted in Section I.A.2.a)(a) or (b)

B. Detection of red flags in an existing account will require the employees to authenticate the customer, monitor the account and/or verify the validity of change of address.

1. Authentication procedures from the CPNI procedures manual will be used, See VI, Safeguards of the Disclosure of CPNI (Authentication) in the CPNI manual.

III. Response to Red Flags: the risk of identity theft will determine what action should be taken in order to prevent or mitigate identity theft.

A. Illustrative measures in response to Red Flags that could be taken may include the following:

1. Monitoring an account for identity theft.

2. Contacting the customer.

3. Changing any passwords, security codes, or other security devises that permit access to a customer account; this could be internal as well as external.

4. Reopening an account with a new account number or telephone number.

5. **Not opening an account.**

6. **Closing an existing account.**

7. **Notifying law enforcement.**

8. **Not attempting to collect on a covered account or not selling a covered account to a debt collector.**

9. **Determining no response is warranted.**

B. Should contact with law enforcement be warranted the Compliance Officer should be contacted immediately and will take the appropriate steps to resolve the issue.

1. **A log will be maintained that includes the date, time, description of the incident, action taken, who the incident was reported to (which law enforcement agency, name of officer taking incident), and action prescribed by law enforcement. (See Exhibit A)**

2. **A log will be maintained by the Compliance Officer to determine if there are any changes of risk of identity in order to update the program.**

IV. Updating the Program: To ensure the Program remains effective over time it will be updated periodically to reflect changes in risks to customers, and to the safety and soundness of the Company from identity theft.

A. The Company will conduct at minimum annual reviews of the program to ensure reflections of any changes in risks of identity theft.

1. **Factors to include in the risk analysis will include:**

   a) ***Company's or personnel's experience(s) with identity theft;***

   b) ***Changes in methods of identity theft;***

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

   d) ***Changes in accounts that it offers or maintains; and***

e) Changes in its business relationships, including mergers, acquisitions, alliances, joint ventures, and service provider arrangements.

B. Administration of the Program: The following describes the steps to administer the Program.

1. The Company must have the Board or committee of the Board approval of the initial written Program.

2. The Company will ensure oversight of the development, implementation and administration of the ongoing Program, by designating a senior management employee to be further referred to as the Compliance Officer.

a) Responsibilities of the Compliance Officer will include:

(a) Implementation of the Program.

(b) Review of reports by staff on compliance.

(c) Approval of material changes to the Program as necessary to address changing identity theft risks.

(d) Preparation of an annual report for the Board's review. Reports must discuss material matters related to the Program and evaluate such issues as:

(a) The effectiveness of the policies and procedures in addressing the risk of identity theft in connection with the opening of accounts and with respect to existing accounts;

(b) Service provider arrangements; review contracts at a minimum annually to ensure service providers have policy and procedures in place to detect, prevent and mitigate identity theft.

(c) Significant incidents involving identity theft and management's response.

(d) Recommendations for changes in the Program.

(e) Implement recommended changes.

(e) Ensure that relevant staff is trained with regard to the Company's Policies and Procedures that detect, prevent and mitigate identity theft and they have signed a Training document to that affect. (See Exhibit B)

(a) Staff will be re-trained annually to ensure they are kept up-to date with the changing risks of identity theft, and will sign a Training document to that affect. (See Exhibit C)

V. Examples of Red Flags by category. The Company will take the appropriate steps to detect, prevent and mitigate relevant Red Flags. This is not an all inclusive list, therefore as more red flags are found the Company will take the appropriate action to update them in their list and have the Compliance Officer include in their annual report in order to update the program accordingly.

A. Alerts, Notifications, or Warnings from a Consumer Reporting Agency. Examples include but are not limited to:

1. A report indicating a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or customer such as; an account that was closed for cause or identified for abuse of account privileges by a creditor.

2. A fraud or active duty alert is included with a consumer report.

3. A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.

4. A consumer reporting agency provides a notice of address discrepancy.

5. A consumer report indicates a pattern of activity not consistent with the history or usual pattern of activity of 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.

B. Suspicious documents, examples include but are not limited to:

1. Documents provided for identification appear to have been altered or forged.

2. The photograph or physical description on the identification is not consistent with the appearance of the customer presenting the identification.

3. Other information on the identification is not consistent with readily accessible information that is on file, such as a signature card or recent check.

4. An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

C. Suspicious personal identifying information

1. Information is inconsistent when compared against external information sources used by the Company. Examples include but are not limited to:

a) The address does not match any address provided on consumer report.

b) The Social Security Number (SSN) has not been issued or is listed on the Social Security Administration's Death Master File.

2. Personal identifying information provided by the customer is not consistent with any other personal identifying information provided by the customer. For example, there is a lack of correlation between the SSN range and date of birth.

3. Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third party sources. Examples include but are not limited to:

a) The address on an application is fictitious, a mail drop, or a prison.

b) The phone number is invalid, or is associated with a pager or answering machine.

4. The SSN is the same as submitted by other persons opening an account.

5. The address or phone number provided is the same as or similar to the account number or telephone number submitted by unusually large number of other persons opening accounts or other customers.

6. The person opening the account fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.

7. Personal identifying information provided is not consistent with information on file with the company.

D. Unusual Use of, or Suspicious Activity related to, the Covered Account; examples include but are not limited to:

1. Shortly following the notice of a change of address the company receives a request for a new, additional, or replacement card or a cell phone, or for the addition of authorized user on the account.

2. An account is used in a manner that is not consistent with established patterns of activity on the account such as;

a) Nonpayment when there is no history of late or missed payments,

b) A material change in telephone call patterns in connection with a cellular phone.

3. An account that has been inactive for a reasonably lengthy period of time is used; take into consideration the type of account, expected pattern of usage and other relevant factors.

4. Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's account.

5. The Company is notified that the customer is not receiving paper account statements.

6. The Company is notified of unauthorized charges or transactions in connection with the customer's account.

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

1. This pertains to when the Company is notified by a customer, a victim of identity theft, a law enforcement authority, or any other person that has opened a fraudulent account for a person engaged in identity theft.

F. Additional possible Red Flags may include:

1. **Repeated attempts to log into account with incorrect passwords.**
2. **Detection of hacking efforts.**
3. **Unauthorized access to electronic or paper records by employees.**
4. **Missing paper records or electronic storage media.**
5. **Break-in at the business office or office maintaining customer identifying information.**

VI. Consumer education.

A. The Company will periodically send a Consumer Privacy Notice, see Exhibit D.

B. Employees will take the initiative to educate the customer as to their privacy rights and the Company's responsibility to ensure that it is in compliance with the Federal Trade Commission and Federal Communications Commission's rules.

1. **Explanation should include discussion as to why it is necessary to authenticate the customer with the necessary documents, passwords and/or security questions.**
2. **The Company will provide a notice stating it requires two pieces of ID, one of which must be a photo ID at all retail locations.**
3. **A copy of the Consumer Privacy Notice will be made publicly available at the Company's retail locations.**

VII. Frequently Asked Questions (FAQ): Questions and responses should be written in the following format. Reference to where the response can be found in the manual provides the tool for employees to be able to refer back to that specific section of the manual for future reference.

Q1:

R1:

Reference: Reference section of the manual that pertains to the question.

EXHIBIT A
LOG OF IDENTITY THEFT INCIDENTS

Date	Time	Description of Incident	Action Taken	Report to Law Enforcement	Signature Compliance Officer/Designee	Date

EXHIBIT B

INITIAL RED FLAGS RULES EMPLOYEE TRAINING VERIFICATION

Date: _____

Employee Name: (Print)_____

I have attended Red Flags training, reviewed the Red Flag Policy and Operating Procedures and agree to comply with the company's policy and procedures set forth therein.

I understand that any infraction of the operating procedures could result in disciplinary action, up to and including termination.

_____

Employee Signature

_____

Supervisor Signature

EXHIBIT C

ANNUAL RED FLAGS RULES AND CPNI EMPLOYEE TRAINING VERIFICATION

Date: _____

Employee Name: (Print)_____

I have attended the annual updated training for Red Flags and CPNI. I have reviewed the updates to the Red Flag and CPNI Policy and Operating Procedures and agree to comply with the company's policy and procedures set forth therein.

I understand that any infraction of the operating procedures could result in disciplinary action, up to and including termination.

_____

Employee Signature

_____

Supervisor Signature

EXHIBIT D

Consumer Privacy Notice

A Commitment to Your Privacy:

S&T and its affiliates, hereinafter the "Company"; consider your privacy and your personal information our number one priority. We are committed to protecting the privacy of information we maintain about you and we want you to be aware of how we collect and handle that information.

Your Privacy is not for sell:

We do not sell or disclose your personal information to anyone, for any reason, at any time. The only exceptions to this would include the following:

- If you specifically authorize us to share your information with another company.
- It is required by law and when we believe that disclosure is necessary to protect our rights and/or to comply with a judicial proceeding, court order, or legal process served on the Company.
- Disclosure is necessary to protect the safety of customers, employees or property.
- Publishing your name, address and phone number in our directories, unless you have requested a non-listed or non-published telephone number.
- Sharing data with our authorized vendors, contractors, and agents, only to the extent necessary for them to perform their work, in order for the Company to carry out certain functions in marketing and delivering services to you.

Should the Company share non-personally identifiable information with non-Company companies in order to assess the results of a promotion or event, the information will be used in the aggregate only, and will not contain any information that would personally identify you.

Personal information you voluntarily supply when obtaining information or purchasing products is not shared for non–Company purposes. This information is Company proprietary data and is not available for use to any outside company in this personalized form. Should any changes be made in the way we use personally identifiable information, the Company will notify you of this change and give you the opportunity to choose to "opt-out" of such use.

How We Collect Information About You: We collect information about you in a number of ways:

- **Application and registration information:** We collect information from you when you open an account or make changes to an existing account. The information we collect includes personal information such as your name, address, phone number, email address, Social Security Number (SSN), driver's license number and date of birth. You will always retain the option to choose if our information is used to send you Company and product information, special offers and in some cases newsletters.
    - **At any time you may:**
        - Elect not to receive (opt-out) marketing messages. The primary purpose of these messages is the commercial advertisement or promotion of a product or service. At any time you may "opt-out".
        - Update your contact and personal information.
- **Transaction and experience information:** Once you have opened an account with us, we collect and maintain personal information about your account, including, transactions, balances, and history. This information allows us to administer your account and provide the services you have requested.
- **Third-party information providers:** We may collect information about you from information services and consumer reporting agencies to verify your identity, employment, or creditworthiness.

Safeguarding Your Information Maintaining Your Trust:

We take precautions to ensure the information we collect about you is protected and is accessed only by authorized individuals or organizations. Companies we use to provide support services are not allowed to use information about our customers for their own purposes and are contractually obligated to maintain strict confidentiality.

We restrict access to personal information by our employees and agents. Our employees are trained about privacy and are required to safeguard personal information.

We maintain physical, electronic and procedural safeguards to protect personal information.

Teaming Up Against Identity Theft:

Identity theft is a serious concern to all of us. Safeguarding information to help protect you from identity theft is a priority with S&T. We are committed to keeping your personal

information safe. To enhance your security, S&T takes steps to protect you from identity theft:

- Utilizing customer identification and authentication procedures before initiating any transactions;
- Using firewalls and encryption technology to protect personal identification on our computer systems;
- Training our employees on privacy and security to properly handle personal information about you.

You can also help protect your identity and accounts.

Here are a few steps to remember:

- When using the internet, keep your login ID and password confidential;
- Keep your security software up-to-date and turned-on;
- Shred documents that contain personal information;
- Check your credit report regularly for unauthorized activity and protect you personal identification numbers (PINs) and personal data.

If you suspect fraud or identity theft, the faster you act the better. Please call your local office:

Brewster 785-694-2256 or 800-432-8294

Colby 785-460-7300 or 866-790-0241

Dighton 620-397-2111 or 877-591-1212

Goodland 785-890-7400 or 866-790-0243

Oakley 785-671-8930