IDENTITY THEFT PREVENTION PROGRAM
NATCO COMMUNICATIONS, INC.
NORTHERN ARKANSAS TELEPHONE CO., INC.
NATCO TECHNOLOGIES, INC.

NATCO Communications, Inc. (NATCO) (includes any related entities, as described in Attachment A hereto) has adopted and implemented this Identity Theft Prevention Program in order to improve its capabilities to detect, prevent and mitigate identity theft with respect to new and existing customer accounts. The core of this Program is the listing of various patterns, practices and specific activities (called "Red Flags") which may indicate the possible theft of the identities of: (a) existing customers maintaining "covered accounts" with NATCO; and (b) new or purported new customers opening "covered accounts" with NATCO. By increasing the awareness and watchfulness of NATCO employees and service providers with respect to such Red Flags, NATCO is attempting to do its part to benefit the public interest by improving its chances of noticing or discovering incidents of potential identity theft in order to help law enforcement and customers prevent the crime and/or mitigate the impacts thereof.

NATCO has also adopted related procedures governing: (a) its use of consumer reports and associated notices of address discrepancies; and (b) its handling of address changes and closely proximate requests for additional or replacement calling, credit or debit cards that it might issue.

This Identity Theft Prevention Program is required by Sections 114 and 315 of the Fair and Accurate Credit Transactions ("FACT") Act of 2003, and by Section 681.2 of the Federal Trade Commission's Rules. These provisions apply to financial institutions and creditors. "Creditors" are defined broadly as entities that regularly extend, renew or continue credit, and appear to include most telecommunications carriers, but can apply to ANY company that extends credit to customers.

It is the official policy of NATCO: (a) to take good faith and reasonable measures to deter the theft of the financial and business identities of customers of the "covered accounts" offered and maintained by NATCO; (b) to make good faith and reasonable efforts to try to notice or discover indications of the possible theft of the financial and business identities of its customers, potential customers and other affected individuals insofar as such actual and attempted identity thefts relate to "covered accounts" offered and maintained by NATCO; and (c) to take reasonable and practicable actions to assist victims of identity theft to minimize and repair damage with respect to such covered customer accounts.

HOWEVER, NATCO DOES NOT PROMISE, GUARANTEE OR WARRANT TO ANY EXISTING, FUTURE OR POTENTIAL CUSTOMER OR TO ANY OTHER INDIVIDUAL OR ENTITY THAT NATCO WILL BE SUCCESSFUL IN OBSERVING OR NOTING THE SIGNIFICANCE OF A RED FLAG IN ANY PARTICULAR

INSTANCE, OR THAT NATCO WILL BE SUCCESSFUL IN ANY PARTICULAR INSTANCE IN DETECTING OR PREVENTING IDENTITY THEFT OR IN MITIGATING INJURY FROM IDENTITY THEFT.

It is the responsibility of NATCO employees and service providers: (a) to review and become familiar with this Program; (b) to be aware of and watchful for Red Flags and other patterns, practices and specific activities that may indicate potential instances of identity theft; (c) to report Red Flags and other suspected identity theft attempts or activities promptly to NATCO's designated Red Flag Coordinator and/or to their immediate supervisors; and (d) to seek clarification from NATCO's Red Flag Coordinator regarding any questions or concerns they have regarding identity theft or this Program.

I. WHAT IS "IDENTITY THEFT"?

Identity theft is the wrongful acquisition of an individual's personal identifying information (such as his or her name, Social Security number, credit card number or other financial account information), and the use of such information without the individual's permission in a manner that involves fraud or deception, typically for economic gain.

There are presently four general categories of identity theft, including: (1) financial identity theft (using another's identity to obtain goods and services); (2) business/commercial identity theft (using another's identity or business name to obtain credit); (3) criminal identity theft (posing as another individual when apprehended for a crime); and (4) identity cloning (using another's information to assume his or her identity in daily life). In addition to damaging an individual's good name and credit rating by the running up of substantial unpaid debts in the victim's name, identity theft can facilitate additional crimes such as blackmail, illegal immigration, terrorism and espionage, as well as enable attacks upon credit card processing, medical insurance and other critical online payment systems.

The theft of personally identifying information can occur in a constantly expanding and changing variety of ways. Some of the current methods include: (a) "dumpster diving," or the rummaging through trash looking for bills or other discarded documents containing personal information; (b) "skimming," or the stealing of credit and debit card numbers via a special storage device when the card is being processed during a transaction; (c) "phishing," or the transmission of spam or pop-up messages seeking personal information by entities pretending to be financial institutions or other trusted businesses; (d) "pretexting," or the use of false pretenses to obtain personal information over the telephone from financial institutions, telephone companies and other businesses; (e) "Trojan horses" and "hacking," or the unauthorized entry into databases to steal personal information; (f) unauthorized "changes of address" to divert billing statements to another location in order to obtain personal information and/or to delay discovery of fraudulent accounts and purchases; (g) "shoulder surfing," or the eavesdropping upon public transactions to obtain personal information; (h) advertising of "bogus job offers" that enable the perpetrators to obtain applications containing personal information; (i) browsing MySpace, Facebook and other online social network sites to obtain posted personal details; and (j) old-fashioned theft of wallets, purses, bank and credit card statements, pre-approved credit offers, new checks, tax information and personnel records. These techniques are constantly changing and expanding.

Once personally identifying information is obtained by an identity thief, it may be used for various fraudulent and deceptive purposes, including to: (1) open credit card accounts in the victim's name; (2) open new wireline or wireless telecommunications service accounts in the victim's name; (3) rent houses and apartments using the victim's name; (4) obtain cable television service in the victim's name; (5) apply for and obtain jobs using the victim's name and Social Security number; (6) obtain medical services in the victim's name; (7) open bank accounts in the victim's name; (8) obtain loans in the victim's name; (9) write bad or counterfeit checks in the victim's name; (9) clone debit or ATM cards in the victim's name and drain the victim's accounts; (10) obtain driver's licenses containing the victim's name and personal information and the identity thief's photo; (11) file fraudulent tax returns in the victim's name; (12) obtain electric, water and other utility services in the victim's name; and (13) use the victim's name and Social Security number to obtain government benefits.

II. WHAT IS A "COVERED ACCOUNT"?

A "covered account" is a continuing relationship: (a) that a financial institution or a creditor (such as a telecommunications company) offers or maintains with a person to facilitate the person's purchase of products or services primarily for personal, family or household purposes; and (b) that involves or is designed to permit multiple payments or transactions. For example, this type of "covered account" would appear to encompass many accounts for residential local exchange, toll, Internet access and/or video services.

A "covered account" also includes any other continuing relationship that a financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk of injury (including risk of financial, operational, compliance, reputation and/or litigation injury) from identity theft: (a) to the customer of the account; or (b) to the safety and soundness of the financial institution or creditor. For example, this type of "covered account" would appear to encompass certain sole proprietor, small business and other business accounts.

As required by the Federal Trade Commission's rules, NATCO has conducted a risk assessment to determine whether it offers or maintains "covered accounts." This risk assessment has taken into consideration: (1) the methods NATCO uses to open its accounts; (2) the methods the NATCO provides to access it accounts; and (3) the nature and extent of the previous experiences (if any) of NATCO with identity theft.

As a result of this risk assessment, NATCO has determined that it has covered residential and/or business accounts, and that it is presently required to implement this written Identity Theft Prevention Program.

NATCO will conduct its risk assessment regarding "covered accounts" every three years, unless and until the FTC defines "periodically" to consist of a longer or shorter period. These future risk assessments are intended to focus primarily upon the potential expansion of NATCO's

"covered accounts" but could result in the elimination or reduction of certain types of "covered accounts" in conjunction with industry experience and future FTC and judicial rulings.

III. ELEMENTS OF NATCO'S IDENTITY THEFT PREVENTION PROGRAM

NATCO's Identity Theft Prevention Program consists of the following four elements:

1. Identification of relevant Red Flags for the covered accounts that NATCO offers.

2. Observation looking toward the potential detection of Red Flags that have been incorporated into the Program.

3. Appropriate responses to detected Red Flags to prevent and mitigate identity theft.

4. Periodic updates to reflect changes in identity theft risks to customers and to NATCO.

IV. IDENTIFICATION OF RELEVANT RED FLAGS

NATCO considers the following four factors in identifying relevant Red Flags for its covered accounts: (1) the types of covered accounts it offers or maintains; (2) the methods that it provides to open its covered accounts; (3) the methods it provides to access its covered accounts; and (4) the nature and extent of its previous experience with identity theft.

At this time, NATCO has incorporated the following Red Flags into its Identity Theft Prevention Program:

A. Alerts, Notifications or Warnings received from a Consumer Reporting Agency

1. A fraud or active duty alert is included with a consumer report, or similar report (e.g., Experian Social Search), for a customer or potential customer.

2. A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report for a customer or potential customer. (Note: As of 5/1/09, NATCO does not subscribe to a full subscriber credit report)

3. A consumer reporting agency provides a notice of address discrepancy for a customer or potential customer (that is, a substantial difference between the address listed for the named consumer in the request for a report on the consumer and the address for the customer in the consumer reporting agency's file). (Note: As of 5/1/09, NATCO does not subscribe to a full subscriber credit report).

4. 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: (Note: As of 5/1/09, NATCO does not subscribe to a full subscriber credit report)

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.

B. Suspicious Documents

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

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

7. Other information on the identification is not consistent with information provided by the person opening a new covered account or by the customer presenting the identification.

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

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

C. Suspicious Personal Identifying Information

10. Personal identifying information provided is inconsistent when compared against external information sources used by NATCO. For example:

a. The address does not match any address in a consumer report, or similar report (e.g., Experian Social Search); or

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

11. 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.

12. Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by NATCO. 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.

13. Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by NATCO. For example:

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

b. The phone number on an application is invalid, or is associated with a pager or answering service.

14. The SSN provided is the same as that submitted by other persons opening an account or other customers.

15. 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.

16. 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.

17. Personal identifying information provided is not consistent with personal identifying information that is on file with NATCO.

18. 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.

D. Unusual Use of, or Suspicious Activity Related to, the Covered Account

19. Shortly following the notice of a change of address for a covered account, NATCO: (a) receives a request for a new, additional, or replacement calling card; (b) receives a request for the addition of authorized users on the account; or (c) notices a significant change in the customer's usage or usage patterns.

20. A new 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.

21. 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;

b. A material increase in the use of available credit; (Note: NATCO presently does not impose credit limits on customers).

c. A material change in call or usage patterns.

22. 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).

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

24. NATCO is notified that the customer is not receiving paper account statements.

25. NATCO is notified of unauthorized charges or transactions in connection with a customer's covered account.

E. Notice from Customers, Victims of Identity Theft, Law Enforcement Authorities, or Other Persons Regarding Possible Identity Theft in Connection With Covered Accounts Held by NATCO

26. NATCO 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.

V. DETECTING RED FLAGS

A. Establishing New Covered Accounts

Upon receiving a telephone or in-person request for the establishment of a new wireline telecommunications service account, NATCO will request and obtain, at a minimum, the following information from the customer before opening the account: (1) full legal name of the customer responsible for payment; (2) date of birth of the responsible customer; (3) for business accounts, the taxpayer identification number for the customer; (4) address at which service is to be provided; and (5) billing address (plus a reasonable and credible explanation for the difference if not the same address as the service address). If a NATCO employee handling the request for the establishment of the new account is not satisfied with the responses to these questions, the employee can request that the customer come in person to NATCO's business office (if not already there) and produce a copy of his or her current driver's license, passport or other reliable government-issued identification. (However, NATCO employees should keep in mind that

people moving into an area often apply for telecommunications or other services before obtaining new or modified driver's licenses to reflect their new addresses.)

NATCO will offer each customer opening a new account the option and opportunity to establish a password to be associated with the account. The new customer will be informed that use of such password is mandatory if the customer wishes: (a) to access his or her account online; (b) to make significant changes in the account (such as changing the billing address and/or adding or changing responsible customers); and/or (c) to request call detail information and other Customer Proprietary Network Information ("CPNI") over the telephone. Those customers electing to establish a password may also establish a back-up "shared secret" customer authentication device by selecting two personal questions and pre-arranged answers to both questions (for example, favorite color, song, book, movie, sports team, and so forth) in order to be able to access their accounts online, obtain CPNI over the telephone, or obtain new passwords if they forget their initial passwords

If NATCO's applicable tariff or service contract permits, NATCO may request and obtain a deposit from a new customer at the time that NATCO establishes a new account or before NATCO commences the provision of service. The amount, terms and condition of such deposit will depend upon the applicable tariff or service contract provisions.

NATCO management has the discretion to order credit reports with respect to some or all customers that open new accounts.

B. Changes to Existing Covered Accounts

NATCO employees need to be aware of the types of changes to existing customer accounts that may indicate potential identity theft activity. At this time, the principal types of such changes include: (a) change of the billing address for an account; (b) change of the responsible customer for an account; and (c) addition of one or more new responsible customers for an account.

Customers who have elected to establish passwords and back-up "shared secret" customer authentication devices will be able to make changes to their existing accounts online or over the telephone. NATCO's employees are not authorized to block such changes if a valid password or shared secret combination is used, but are required to report suspicious changes regarding existing accounts promptly to the Red Flag Coordinator and/or to their supervisors.

Customers who have not established passwords and back-up "shared secret" customer authentication devices will be able to change the billing address and/or responsible customer for an account, or add one or more new responsible customers, only if: (a) the existing responsible customer comes in person to NATCO's billing office and produces a driver's license, passport or other government-issued identification sufficient to verify his or her identity; or (b) the existing responsible customer calls NATCO from the wireline or wireless telephone associated with the subject existing account, requests the change, and then terminates the call and is called back at that number by NATCO's employee.

The Federal Communications Commission's ("FCC's) CPNI Rules, which apply to telecommunications carriers and supplement the FCC's Red Flag rules, require NATCO to notify customers immediately of certain changes in their accounts that may affect privacy or security matters. The types of changes that require immediate notification include: (a) a change or request for change of the customer's password; (b) a change or request for change of the customer's address of record; (c) a change or request for change of any significant element of the customer's online account; and (d) a change or request for change to the customer's back-up "shared secret" questions and answers. The notice may be provided by: (a) a NATCO call or voicemail to the customer's telephone number of record; (b) a NATCO text message to the customer's telephone number of record; or (c) a written notice mailed to the customer's address of record (NOTE: to the customer's prior address of record if the change includes a change in the customer's address of record). The notice must identify only the general type of change and must not reveal the changed information.

NATCO is aware that changes of billing addresses or responsible customers to allow adult children (or other relatives or friends) of elderly customers to pay bills and monitor accounts constitute very sensitive areas. NATCO recognizes the need to allow legitimate representatives of elderly customers to assist with the handling of their services, bills and accounts without forcing such representatives to travel hundreds or thousands of miles to appear in person at NATCO's office. At the same time, NATCO is concerned that criminals who prey upon elderly people may pose as adult children, relatives or friends to gain unauthorized access to the accounts and identities of elderly customers for fraudulent purposes. NATCO will follow a policy of vigilant flexibility in dealing with these situations. NATCO employees will normally respond to requests for changes of billing addresses and/or responsible customers on behalf of elderly customers: (a) by requiring the adult child, relative or friend to furnish proof via a legally binding power of attorney or similar notarized and valid legal document that he or she is authorized by the elderly customer to transact business on his or her behalf; or (b) by having the elderly customer confirm via telephone from his or her telephone number of record (or via a three-way call including the elderly customer from his or her telephone number of record and the adult child, relative or friend) that he or she intends to make the change. If these approaches are not practicable in light of the special needs and circumstances of a particular elderly customer or if a NATCO employee is concerned that identity theft or other fraud may be taking place, the NATCO employee must bring the matter to the attention of NATCO management (including the Red Flag Coordinator and the CPNI Compliance Officer). Management (in consultation with counsel, if necessary) may devise specific alternative solutions to meet the legitimate account revision needs of elderly customers while protecting them against identity theft (for example, by working with reputable clergy, doctors, nurses and/or social workers who are familiar with the elderly customer's circumstances and desires).

NATCO management has the discretion to place certain covered accounts on a "watch list" where they will be monitored on a regular basis for a reasonable period after a change of billing address and/or responsible customer for the account, and/or the addition of one or more new responsible customers.

VI. RESPONSES TO PREVENT AND MITIGATE IDENTITY THEFT

If a NATCO employee observes one or more of the Red Flags listed in Section IV above, the employee is required to bring the matter promptly to the attention of NATCO's designated Red Flag Coordinator and/or the employee's immediate supervisor (who shall, in turn, bring the matter promptly to the attention of the Red Flag Coordinator or an appropriate NATCO officer or management-level employee if the Red Flag Coordinator is unavailable). A report will generally be considered to be "prompt" if made during the same business day that the Red Flag was observed or during the following business day. Initial reports may be made orally, but must be followed-up by a written memorandum or email detailing the Red Flag observation (including a description of the Red Flag, name of customer or purported customer, name of observing employee, and time and date of observation) before the end of the following business day.

Upon being informed of the observation of a Red Flag, the Red Flag Coordinator will consult with designated members of NATCO's officers and upper-level management to determine the nature and degree of identity theft risk posed by the observed Red Flag(s) and take action as appropriate.

Any specific company reporting procedure to be followed upon discovery of a Red Flag will be set forth in Attachment A to this Policy, as may be amended from time to time.

NATCO's response to a Red Flag situation may include, but not be limited to:

1. Monitoring the affected covered account(s) for evidence of identity theft;

2. Contacting the affected customer(s);

3. Changing any passwords, security codes, or other security devices that permit access to the affected covered account(s);

4. Reopening an affected covered account/telephone number with a new account/telephone number;

5. Not opening a new covered account;

6. Closing an existing covered account;

7. Not attempting to collect on an affected covered account, or not selling the covered account to a debt collector;

8. Notifying law enforcement; or

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

NOTE: In determining an appropriate response, NATCO and its employees will consider the presence of any aggravating factors that may heighten the risk of identity theft. For example, such aggravating factors may include: (a) the occurrence of a recent data security breach that resulted in known or suspected unauthorized access to NATCO's account records; (b) a notice from a customer that he or she has provided his or her account information to someone who fraudulently claimed to represent NATCO; and (c) a notice from a customer that he or she may have provided personal or account information to a fraudulent website in a phishing scam.

CAUTION: NATCO and its employees will act in good faith and exercise reasonable efforts to try to observe and note the significance of Red Flags, and to take appropriate action(s) to detect, prevent and mitigate identity theft when one or more Red Flags are observed. However, identity theft is a very complex and changing crime perpetrated by clever and inventive criminals, and is often very difficult to detect before significant damage is done to the victim. **NATCO does not promise or guarantee to any existing, future or potential customer that it will able to observe and note the significance of a Red Flag in any particular instance, or that it will be successful in any particular instance in detecting or preventing identity theft or in mitigating injury from identity theft.**

VII. PERIODIC UPDATES TO PROGRAM

This Identity Theft Prevention Program must be reviewed and updated "periodically" to reflect: (a) changes in identity theft risks regarding the "covered accounts" of customers; (b) changes in the Red Flags determined to be relevant to such risks; and (c) changes in identity theft risks to the safety and soundness of NATCO.

Program reviews and updates will be based upon factors such as:

1. The nature and extent of the experience of NATCO with identity theft;

2. Changes in methods of identity theft;

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

4. Changes in the types of accounts that NATCO offers; and

5. Changes in the business arrangements of NATCO (including mergers, acquisitions, alliances, joint ventures, and service provider arrangements).

NATCO's Board of Directors will initiate and supervise a review and update of the Program: (a) if NATCO discovers three or more instances of identity theft during a calendar quarter that were not able to be detected, prevented and/or mitigated by the existing provisions of the Program; (b) if the annual Identity Theft Prevention Program Compliance Report to NATCO's Board of Directors recommends that a periodic review and update be conducted; or (c) at the end of the

third year after the last periodic review and update (unless and until the FTC defines "periodically" to consist of a longer or shorter period).

VIII. DUTIES OF NATCO WHEN USING CONSUMER REPORTS

When NATCO uses consumer reports or similar reports, (e.g., Experian Social Search) and determines there is an address discrepancy with respect to a particular report, NATCO will use the following methods to form a reasonable belief that the report relates to the consumer about whom it has requested the report:

1. Compare the information in the report provided by the reporting agency with the information NATCO maintains in its own records or obtains from third party sources; or

2. Verify the information provided by the reporting agency with the consumer.

IX. DUTIES OF CALLING, CREDIT OR DEBIT CARD ISSUERS REGARDING CHANGES OF ADDRESS

This Section IX applies only if NATCO issues calling, credit or debit cards.

NATCO receives notification of a change of address from a card holder and then, within 30 days after it receives such notification, NATCO receives a request for an additional or replacement card for the same account, NATCO will not issue an additional or replacement card until it has:

1. Notified the cardholder of the request: (a) at the cardholder's former address; or (b) by other means that NATCO and the cardholder have previously agreed to use (NOTE: This notice must be clear and conspicuous and provided separately from NATCO's regular correspondence with the cardholder); and

2. Provided to the cardholder a reasonable means to promptly report incorrect address changes.

X. ADMINISTRATION OF PROGRAM

NATCO's Board of Directors has approved and adopted this initial Identity Theft Prevention Program, and has required it to be implemented and effective as of November 1, 2008.

The Board of Directors must review, approve and adopt any and all revisions and modifications to this Identity Theft Prevention Program.

NATCO's Red Flag Coordinator appointed by the Board of Directors is shown in Attachment A.

The Red Flag Coordinator is responsible for the implementation and day-to-day supervision of NATCO's Identity Theft Prevention Program. These duties include: (a) preparation and presentation of an annual written Identity Theft Prevention Program Compliance Report to the

Board of Directors; (b) training NATCO employees regarding their responsibilities with respect to the Program and responding to employee questions and concerns regarding identity theft or the Program; (c) consultation with designated members of the NATCO's officers and upper-level management, and the selection and execution of appropriate action in response to the discovery of one or more Red Flags; and (d) oversight of the NATCO's service providers with respect to identity theft matters.

XI. ANNUAL COMPLIANCE REPORT

The Red Flag Coordinator must prepare (or supervise the preparation) and present to the Board of Directors each year (by the date specified in Attachment A) an annual written Identity Theft Prevention Program Compliance Report. The Compliance Report must contain descriptions and evaluations of:

1. The effectiveness of the policies and procedures of NATCO's Program in addressing the risk of identity theft: (a) in connection with the opening of covered accounts; and (b) with respect to existing covered accounts;

2. The nature and extent of NATCO's service provider arrangements, and their impact upon the effectiveness of NATCO's Program;

3. Significant incidents involving identity theft and NATCO's responses to such incidents; and

4. Recommendations (if any) that a periodic review be conducted (see Section VII) under the supervision of the Board of Directors to consider the adoption of material changes and other revisions, modifications and updates to the Program.

XII. TRAINING OF EMPLOYEES

The Red Flag Coordinator will supervise the training of all employees who are likely to deal with new and/or existing covered accounts of customers and who may be in a position to notice Red Flags indicating potential identity theft. These employees may include: (a) officers and managers; (b) customer service and account representatives; (c) sales and marketing representatives; (d) billing and collection personnel; and (e) accounting and bookkeeping personnel.

All such employees must receive, read and review a copy of this Identity Theft Prevention Program. Each such employee must then attend a group training session (or, if timing and/or other circumstances render attendance at a group training session impracticable, a private meeting) with the Red Flag Coordinator during which the Program will be reviewed, discussed and clarified.

The Red Flag Coordinator will conduct follow-up training sessions: (a) for new or existing employees who assume new job responsibilities that are likely to bring them into contact with

new and/or existing covered accounts of customers; (b) if and when material changes and other substantial revisions, modifications and updates are made to the Program; and/or (c) periodically when NATCO management and the Red Flag Coordinator believe that a refresher training session is needed to remind employees of identity theft issues and/or Red Flag matters.

If they are deemed useful, the Red Flag Coordinator may periodically place notices or reminders of identity theft issues and/or Red Flag matters on internal employee bulletin boards and/or in internal employee newsletters.

XIII. RESPONSE TO DISCOVERY OF RED FLAGS

The Red Flag Coordinator: (a) must be informed promptly (both orally and in writing) by employees and/or their supervisors of the discovery of actual or suspected Red Flags; (b) must consult with NATCO's officers and upper-level management as shown in Attachment A with respect to the selection of the appropriate action(s) to be taken in response to the discovery of such Red Flag(s); and (c) must supervise the implementation of such action(s).

The procedures to be followed and potential actions to be taken by NATCO to try to prevent and mitigate identity theft in response to the discovery of one or more Red Flags are set forth in Section VI ("RESPONSES TO PREVENT AND MITIGATE IDENTITY THEFT") of this Program.

XIV. OVERSIGHT OF SERVICE PROVIDERS

The Red Flag Coordinator must coordinate with third party service providers (such as billing and collection agents and marketing companies) that perform activities on behalf of NATCO in connection with NATCO's new and/or existing covered accounts so as to ensure that the activities of each such service provider are conducted in accordance with reasonable policies and procedures designed to detect, prevent and mitigate the risk of identity theft.

If a service provider has adopted and implemented its own identity theft prevention program and such program is reasonably consistent with NATCO's Program, the Red Flag Coordinator will: (a) request a copy of the service provider's identity theft prevent program for his or her files; (b) request and obtain written assurance (in the form of a letter, email, or a contract amendment, supplement or addendum) from the service provider stating that the service provider will follow its own identity theft prevention program with respect to the activities it performs regarding NATCO's covered accounts; and (c) require the service provider to notify NATCO's Red Flag Coordinator promptly of any Red Flags that the service provider's employees notice or discover with respect to NATCO's covered accounts.

If a service provider has not adopted and implemented its own identity theft prevention program or if such program is not reasonably consistent with NATCO's Program, the Red Flag Coordinator will: (a) provide the service provider with a copy of NATCO's Program; (b) request and obtain written assurance (in the form of a letter, email, or a contract amendment, supplement or addendum) from the service provider stating that the service provider will require its

employees that deal with NATCO's covered accounts to be familiar with NATCO's Program and that the service provider will follow NATCO's Program with respect to the activities it performs regarding NATCO's covered accounts; and (c) require the service provider to notify NATCO's Red Flag Coordinator promptly of any Red Flags that the service provider's employees notice or discover with respect to NATCO's covered accounts.