Star Buick GMC – Star Buick GMC Cadillac – Star Pre owned of Hellertown

Identity Theft Prevention Program

Star's Response to the Detection of Relevant Red Flags: General Policy Our Dealership is committed to identifying relevant Red Flags and responding appropriately to those relevant Red Flags with the purpose of preventing and/or mitigating potential and actual identity theft. Our methods of detection and response are commensurate with the potential level of risk. In responding appropriately to those Red Flags, the Dealership takes into account aggravating circumstances or facts that may increase the risk of identity theft, such as a breach of our computer security measures that results in unauthorized access to customer's non-public account information or actual theft of customer information.

Purpose

The purpose of the program is to establish an Identity Theft Prevention Program (ITPP). It is designed to detect, prevent and mitigate identity theft in connection with existing covered accounts that are being handled for collections under our outsourcing programs or our contingency based programs along with any accounts purchased from creditors with no plans on extending any additional credit. We will provide for continued administration of the ITPP in compliance with Part 681 of Title 16 of the Code of Federal Regulations implementing Sections 114 and 315 of the Fair and Accurate Credit Transactions Act (FACTA) of 2003.

Definitions

Covered account means:

1. An account that a creditor offers or maintains, primarily for personal, family, or household purposes that involves or is designed to permit multiple payments or transactions
2. Any other account that the creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the creditor from identity theft, including financial, operational, compliance, reputation or litigation risks.

Credit means the right granted by a creditor to a debtor to defer payment of debt or to incur debts and defer its payment or to purchase property or services and defer payment therefore.

Creditor means 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.

Identifying information is any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including: name, address, telephone number, Social Security number, date of birth, government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number, unique electronic identification number, computer's Internet Protocol (IP) address, or routing code.

Identity theft means fraud committed or attempted using the identifying information of another person without authority.

Red flag means a pattern, practice or specific activity that indicates the possible existence of identity theft.

Professional Recovery Personnel, Inc. establishes an Identity Theft Prevention Program (ITPP) to detect, prevent and mitigate identity theft. The ITPP shall include reasonable policies and procedures to:

1. Identify relevant red flags for covered accounts it maintains and incorporate those red flags into the

ITTP;

2. Detect red flags that have been incorporated into the ITTP;
3. Respond appropriately to any red flags that are detected to prevent and mitigate identity theft; and
4. Ensure the ITTP is updated periodically to reflect changes in risks to customers and to the safety and soundness of the creditor and or client from identity theft.

The ITTP shall, as appropriate, incorporate existing policies and procedures that control reasonably foreseeable risks.

Identification of Relevant Red Flags

In order to identify relevant Red Flags, the company considers the types of accounts that it maintains, the methods it provides to open its accounts for collection, the methods it provides to access its accounts through eLend On-Line Access over the internet and its previous experience with Identify Theft. The company identifies the following red flags, in each of the listed categories:

A. Notifications and Warnings from Credit Reporting Agencies

- Report of fraud accompanying a credit report;
- Notice or report from a credit agency of a credit freeze on a customer;
- Indication from a credit report of activity that is inconsistent with a customer's usual pattern or activity.

B. Suspicious Documents

- Identification document or card that appears to be forged, altered or inauthentic;
- Identification document or card on which a person's photograph or physical description is not consistent with the person presenting the document;
- Other document with information that is not consistent with existing customer information (such as if a person's signature on a check appears forged); and
- Application for service or credit that appears to have been altered or forged for identity theft.

C. Suspicious Personal Identifying Information

- Identifying information presented that is inconsistent with other information the customer provides (example: inconsistent birth dates);
- Identifying information presented that is inconsistent with other sources of information (for instance, an address not matching an address on the credit report);
- Identifying information presented that is the same as information shown on other applications that were found to be fraudulent;
- Identifying information presented that is consistent with fraudulent activity (such as an invalid phone number or fictitious billing address);
- Social Security number presented that is the same as one given by a client on a different account name;
- An address or phone number presented that is the same as that of another person;
- A person fails to provide complete personal identifying information on an application when reminded to do so (however, by law social security numbers must not be required); and
- A person's identifying information is not consistent with the information that is on file for the customer.

D. Suspicious Account Activity or Unusual Use of Account

- Change of address for an account followed by a request to change the account holder's name;
- Theft of media in transit;

- Breach in the company's computer system security; or
- Unauthorized access to or use of customer account information.

E. Alerts from Others

- Notice to the company from a customer, identity theft victim, law enforcement or other person that it has opened or is maintaining a fraudulent account for a person engaged in Identity Theft.

Detection of Red Flags

Existing Accounts

In order to detect any of the Red Flags identified above for an existing account, PRP will take the following steps to monitor transactions with an account:

- Verify the identification of customers if they request information, whether in person, via telephone, via facsimile or via e-mail;
- Verify the validity of requests to change billing addresses; and
- Verify changes in banking information given for billing and payment purposes.

Response to suspected identity theft

In the event PRP detects any identified Red Flags, such personnel shall take one or more of the following steps, depending on the degree of risk posed by the Red Flag:

- Continue to monitor an account for evidence of Identify Theft;
- Contact the customer:
- Change any passwords or other security devices that permit access to accounts;
- Advise client to close any existing accounts;
- Reopen an account with a new account number;
- Notify the Program Administrator for determination of the appropriate step(s) to take;
- Notify law enforcement; or
- Determine that no response is warranted under the circumstances.

To further prevent the likelihood of identity theft occurring with respect to accounts that are being handled for collection, PRP will take the following steps with respect to its internal operating procedures to protect customer identifying information:

- Ensure that its website is secure;
- Ensure complete and secure destruction of paper documents and computer files containing customer information;
- Ensure that the office computers are password protected and that computer screens lock after a set period;
- Keep offices clear of papers containing customer information;
- Ensure computer virus protection is up to date; and
- Require and keep only the kinds of customer information that are necessary for collection purposes

.

Updating the ITPP

The ITPP shall be updated periodically to reflect changes in risks to customers or to the safety and soundness of the organization from identity theft based on factors such as:

- The experiences of the organization 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 organization maintains;
- Changes in the business arrangements of the organization, including mergers, acquisitions, alliances, joint ventures and service provider arrangements.

Administration of ITPP

- Robert P. Grow, Jr., Business & Personnel Development Director shall be responsible for the development, implementation, oversight and continued administration of the ITPP until further notice.
- The ITPP shall train staff, as necessary, to effectively implement the Program; and
- The ITPP shall exercise appropriate and effective oversight of service provider arrangements.

Oversight of the ITPP

1. Oversight of the ITPP shall include:

a. Review of reports prepared by staff regarding compliance; and

b. Approval of material changes to the ITPP as necessary to address changing risks of identity theft.

2. Reports shall be prepared on the following:

- The effectiveness of the policies and procedures in addressing the risk of identity theft in connection with the existing covered accounts;
- Service provider agreements;
- Significant incidents involving identity theft and management's response; and
- Recommendations for material changes to the ITPP.

Oversight of Service Provider Arrangements

In the event the company engages a service provider to perform an activity in connection with one or more accounts, it will take the following steps to ensure the service provider performs its activity in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of Identity Theft:

- Require, by contract, that service providers have such policies and procedures in place; and
- Require, by contract, that service providers review the company's ITPP and report any Red Flags to the Program Administrator.