

IDENTITY THEFT PREVENTION PROGRAM

_____ [Dealer Name]

1. PROGRAM SUMMARY AND PURPOSE

On November 9, 2007, the Federal Trade Commission (“FTC”) and other federal regulatory agencies published the final rule regarding Identity Theft Red Flags and Address Discrepancies (“Red Flags Rule”) pursuant to the Fair and Accurate Credit Transactions Act of 2003 (the “FACT Act”). See 16 C.F.R. Part 681. The Red Flags Rule requires retailers such as _____ [enter dealer name] (“DEALER”) to develop and implement no later than August 1, 2009, a written Identity Theft Prevention Program that is designed to detect, prevent, and mitigate Identity Theft of consumer information in connection with a Covered Account.

Pursuant to the Red Flags Rule and the FACT Act, DEALER adopts the following Identity Theft Prevention Program (“Program”) to: (1) identify relevant Red Flags for the Covered Accounts that DEALER offers or maintains, and incorporate those Red Flags into this Program; (2) detect Red Flags that have been incorporated into the Program; (3) respond to any Red Flags that are detected to prevent and mitigate Identity Theft; and (4) ensure the Program is updated periodically, to reflect changes in risks to customers.

2. DEFINITIONS

2.1. “Covered Account” means an account that DEALER offers or maintains, primarily for personal, family or household purposes, that involves or is designed to permit multiple payments or transactions; and any other account that DEALER offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of DEALER from Identity Theft, including financial, operational, compliance, reputation, or litigation risks.

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

2.3. “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.

2.4. “Identity Theft” means a fraud committed or attempted using the Identifying Information of another person without authority.

2.5. “Red Flag” means a pattern, practice, or specific activity that indicates the possible existence of Identity Theft.

3. IDENTIFICATION OF ACCOUNTS SUBJECT TO RED FLAG POLICY

DEALER is a retail motorcycle dealership engaged in selling and/or servicing motorcycles, all terrain vehicles, and other types of recreational vehicles. From time to time DEALER may extend credit or defer payment for products or services, or assist customers in obtaining credit or filling out a credit application. DEALER may open or maintain customer accounts for these purposes. After considering the methods it uses to open its accounts, the methods it provides to access its accounts, and its prior experience with Identity Theft, DEALER has determined that it may offer or maintain accounts that may be classified as Covered Accounts to which the Program applies.

4. IDENTIFYING RELEVANT RED FLAGS

4.1. Risk Factors. In establishing the events and occurrences that shall be considered Red Flags for purposes of this Program, DEALER examined its Covered Accounts, including the methods by which DEALER opens and grants access to the Covered Accounts and DEALER's past experience with Identity Theft.

4.2. Sources of Red Flags. In incorporating relevant Red Flags into this Program, DEALER has considered, and will continue to consider in its annual review of the Program, incidents of Identity Theft that DEALER may experience; methods of Identity Theft that reflect changes in Identity Theft risks; and supervisory guidance from consumer protection authorities, such as the guidelines initially published with the FTC's Red Flag Rule.

4.3. Categories of Red Flags. DEALER has identified the following relevant Red Flags that could be associated with the Covered Accounts that DEALER opens or maintains:

4.3.1. Alerts, Notifications, and Warnings. Alerts, notifications, or other warnings received from consumer reporting agencies or Service Providers, such as fraud detection services, can be Red Flags for Identity Theft. Such Red Flags include:

- a. A fraud or active duty alert is included in a consumer report;
- b. A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report;
- c. A consumer reporting agency provides a notice of address discrepancy; and
- d. A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of a customer, such as:
 1. A recent and significant increase in the volume of inquiries;
 2. An unusual number of recently established credit relationships;
 3. A material change in the use of credit, especially with respect to recently established credit relationships; or
 4. An account that was closed for cause or identified for abuse of account privileges.

4.3.2. Suspicious Documents. The presentation of suspicious documents can be a Red Flag for Identity Theft. Such Red Flags include:

- a. Documents provided for identification appear to have been altered or forged;
- b. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification;
- c. Other information on the identification is not consistent with information provided by the person opening a new Covered Account or customer presenting the identification;
- d. Other information on the identification is not consistent with readily accessible information that is on file with DEALER, such as an application for credit or purchase and sale agreement; and
- e. An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

4.3.3. Suspicious Personal Identifying Information. The presentation of suspicious personal Identifying Information, such as a suspicious address change, can be a Red Flag for Identity Theft. Such Red Flags include:

- a. Personal Identifying Information provided is inconsistent when compared against external information sources used by DEALER. For example:
 1. The address does not match any address in the consumer report; or
 2. The social security number has not been issued, or is listed on the Social Security Administration's Death Master File;
- b. 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 social security number range and date of birth;
- c. Personal Identifying Information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by DEALER. For example:
 1. The address on an application is the same as the address provided on a fraudulent application; or
 2. The phone number on an application is the same as the number provided on a fraudulent application;
- d. Personal Identifying Information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by DEALER. For example:
 1. The address on an application is fictitious, a mail drop, or a prison; or
 2. The phone number is invalid, or is associated with a pager or answering service;

- e. The social security number provided is the same as that submitted by other persons opening a Covered Account or other customers;
- f. 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 Covered Accounts or other customers;
- g. 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;
- h. Personal Identifying Information provided is not consistent with personal Identifying Information that is on file with DEALER; and
- i. To the extent DEALER uses a challenge question to confirm a customer's identity, 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.

4.3.4. Suspicious Activity. The unusual use of, or other suspicious activity related to, a Covered Account is also a Red Flag for potential Identity Theft. Such Red Flags include:

- a. Shortly following the notice of a change of address for a Covered Account, DEALER receives a request for the addition of authorized users on the Covered Account;
- b. A Covered Account is used in a manner commonly associated with known patterns of fraud, such as the customer fails to make the first payment or makes an initial payment but no subsequent payments
- c. A Covered Account is used in a manner that is not consistent with established patterns of activity on the account, such as nonpayment when there is no history of late or missed payments.
- d. Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's Covered Account;
- e. DEALER is notified that the customer is not receiving paper account statements;
- f. DEALER is notified of unauthorized charges or transactions in connection with the customer's Covered Account; and
- g. A customer requests that DEALER provide the customer with Identifying Information from DEALER's records.

4.3.5. Notices. Notices of potential Identity Theft are also serious Red Flags. Such Red Flags include:

- a. Notice from a customer of unauthorized charges in connection with that customer's Covered Account;
- b. Notice from customers, law enforcement authorities, or other persons indicating that a customer has been a victim of Identity Theft;

- c. Notice to DEALER that a customer has provided information to someone fraudulently claiming to represent DEALER;
- d. Notice to DEALER that a fraudulent website that appears similar to DEALER's website is being used to solicit customers' Identifying Information; and
- e. DEALER's mail servers are receiving returned e-mails that DEALER did not send, indicating that its customers may have received a fraudulent e-mail soliciting customers' Identifying Information.

4.3.6. Other Relevant Red Flags. There are additional activities that may be Red Flags for Identity Theft relevant to this Program, including:

- a. The name of an employee of DEALER has been added as an authorized user on a Covered Account;
- b. An employee has accessed or downloaded an unusually large number of customer account records;
- c. DEALER detects attempts to access a customer's Covered Account by unauthorized persons; and
- d. DEALER detects, or is informed of, unauthorized access to a customer's Identifying Information.

5. DETECTING RED FLAGS

5.1. Existing Accounts. To detect any of the Red Flags identified above for an existing account, DEALER's personnel will take the following steps:

- a. Monitor transactions and inquiries relating to a Covered Account for suspicious activity;
- b. Verify the identification of customers if they request information, whether in person, via telephone, via facsimile or via e-mail;
- c. Verify the validity of requests to change billing addresses or other information on a Covered Account; and
- d. Verify changes in banking information given for billing and payment.

5.2. New Accounts. To detect any of the Red Flags identified above associated with the opening of a new account, DEALER's personnel will take one or more of the following steps to obtain and verify the identity of the person opening the account:

- a. Require certain identifying information such as name, date of birth, residential or business address, principal place of business for an entity, driver's license or other identification;
- b. Verify the customer's identity (for instance, review a driver's license or other identification card);
- c. Review documentation showing the existence of a business entity; or
- d. Independently contact the customer.

6. PREVENTING AND MITIGATING IDENTIFY THEFT

6.1. Internal Procedures to Prevent Identity Theft. To prevent the likelihood of identity theft occurring with respect to Covered Accounts, DEALER will take the following steps with respect to its internal operating procedures to protect customer Identifying Information:

- a. Ensure that its website is secure or provide clear notice that the website is not secure;
- b. Ensure complete and secure destruction of paper documents and computer files containing customer information;
- c. Ensure that office computers are password protected and that computer screens lock after a set period of time;
- d. Keep offices clear of papers containing customer information;
- e. Request only the last 4 digits of social security numbers (if any);
- f. Ensure computer virus protection is up to date; and
- g. Require and keep only the kinds of customer information that are necessary for business purposes.

6.2. Response to Red Flag Detection. DEALER is committed to preventing Identity Theft. If DEALER detects a Red Flag, DEALER will take the appropriate steps to prevent and mitigate any harm that could be caused by the Red Flag. In responding to a Red Flag, DEALER shall consider aggravating circumstance(s) that may heighten the risk of Identity Theft. After assessing the risk posed, DEALER will respond to the Red Flag in an appropriate manner, which may include:

- a. Monitoring a Covered Account for evidence of Identity Theft;
- b. Contacting or notifying the customer;
- c. Requiring the customer to appear in person with appropriate identification;
- d. Changing any passwords, security codes, or other security devices that permit access to a Covered Account;
- e. Reopening a Covered Account with a new account number;
- f. Not opening a new Covered Account;
- g. Closing an existing Covered Account;
- h. Not attempting to collect on a Covered Account or not selling a Covered Account to a debt collector;
- i. Notifying law enforcement; or
- j. Determining that no response is warranted under the particular circumstances.

6.3. Service Providers. DEALER may have business relationships with service providers who may have access to customers' Identifying Information. For the protection of customers, DEALER shall ensure that the service provider's work for DEALER is consistent with this Program by (a) entering a contract with the service provider that incorporates the Program's requirements; (b) amending a contract with the service provider to incorporate these requirements; (c) if a contract cannot be amended, providing notice of DEALER's

Program to the service provider and request that the service provider comply with the Program; or (d) otherwise determine that the service provider has reasonable alternative safeguards that meet or exceed the level of protection provided by this Program.

7. PROGRAM UPDATES AND ADMINISTRATION

7.1. Updates. DEALER is committed to maintaining an Identity Theft Prevention Program that is current with the ever-changing crime of Identity Theft. To that end, DEALER shall reassess this Program on at least an annual basis to determine whether changes are necessary to reflect changes in risks to customers or to the safety and soundness of DEALER or customers from Identity Theft. In reassessing the Program, DEALER shall consider:

- a. DEALER's past 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 the types of accounts offered or maintained by DEALER; and
- e. Changes in DEALER's business arrangements, including mergers, acquisitions, alliances, joint ventures, and service provider arrangements.

7.2. Administration. Administration of this Program shall be as follows:

7.2.1. Ultimate Authority. The _____ [enter Board of Directors/President/Owner of dealer, etc.] has adopted this Program and will have ultimate authority over the Program.

7.2.2. Oversight. The Program shall be managed by _____ [enter a senior management level position, such as a manager, controller, president, CEO, etc.], who has authority to delegate oversight and compliance to other employees and is responsible for training and reviewing staff and for preparing reports regarding compliance with the Program.

7.2.3. Reports and Records. The _____ [enter senior management position], with the assistance of any personnel assigned responsibility for this Program, shall prepare a report, at least annually, regarding the implementation, progress of, and proposed changes to the Program, if any. The _____ [enter senior management position] shall present the report to the _____ [enter Board of Directors/President/Owner of dealer that has ultimate authority] for review at least annually. The report shall address material matters related to the Program and evaluate issues such as: the effectiveness of the Program 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 management's response; and recommendations for material changes to the Program.

8. ADDRESS DISCREPANCY REQUIREMENTS

8.1. Address Discrepancies. In the event DEALER uses consumer reports, at least one of the following steps must be taken when DEALER receives notice from any consumer reporting agency that a substantial difference exists between the address for the customer that DEALER has been provided and the address(es) in the consumer reporting agency's file for that particular customer:

- a. Compare the differing address with DEALER's file in one of the following ways:
 1. Confirm that the address information provided to DEALER is the same information DEALER obtains and uses to verify the customer's identity in accordance with the requirements of the Customer Information Program (CIP) rules located at 31 C.F.R. 103.121;
 2. Compare the differing address with DEALER's records and files, including applications, change of address notifications, other customer account records, or retained CIP documentation;
 3. Compare the differing address with information DEALER may have received from a third-party source; or
- b. Verify the information in the consumer report provided by the consumer reporting agency with the customer.

8.2. Address Confirmation. To ensure that DEALER maintains and furnishes to a consumer reporting agency accurate address information for its customers, at least one of the following steps must be taken prior to providing service:

- a. Verify the address with the customer about whom DEALER has requested a report;
- b. Review its own records to verify the address of the customer;
- c. Compare the address with information received from a third-party source; or
- d. Verify by other means that are reasonably available at the time.

[END OF PROGRAM]