

IDENTITY THEFT PREVENTION PROGRAM

I. PROGRAM PURPOSE AND DEFINITIONS

A. Purpose

The *YOSKOVICH FUNERAL HOME* ("Funeral Home") developed this Identity Theft Prevention Program ("Program") pursuant to the Federal Trade Commission's Red Flags Rule ("Rule"), which implements Sections 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003 ("FACTA"). This Program was established to detect, prevent, and mitigate identity theft in connection with the opening of an account and the maintenance of an existing account. The Program provides continued administration of the Program in compliance with FACTA

B. Fulfilling requirements of the Red Flags Rule

Under the Red Flags Rule, every creditor is required to establish an identity theft prevention program tailored to its size, complexity and the nature of its operation. The program must contain reasonable policies and procedures to:

1. Identify relevant Red Flags as defined in the Rule and this Program for new and existing covered accounts and incorporate those Red Flags into the Program;
2. Detect Red Flags that have been incorporated into the Program;
3. Respond appropriately to any Red Flags that are detected to prevent and mitigate identity theft; and
4. Update the Program periodically to reflect changes in risks to customers or to the safety and soundness of the *Yoskovich Funeral Home* from identity theft.

C. Red Flags Rule definitions used in this Program

For the purposes of this Program, the following definitions apply:

1. **Account**. "Account" means a continuing relationship established by customer with the *Yoskovich Funeral Home* to obtain products or services including but not limited to:
 - a. At-need or pre-need multiple payment plans maintained by the *Funeral Home or Cemetery*.
 - b. At-need or pre-need accounts paid on credit terms and either opened by the *Funeral Home* or opened with the assistance of the *Yoskovich Funeral Home*.
 - c. Pre-Need account opened with an insurance company allowing the customer to purchase a policy and make installment payments.
 - d. Any other account the *Yoskovich Funeral Home* offers or maintains for which there is a reasonably foreseeable risk to customers from Identity Theft.
2. **Creditor**. "Creditor" has the same meaning as defined in Section 702 of the Equal Credit Opportunity Act, 15U.S.C. 1691a, and includes a person or entity that arranges for the extension, renewal or continuation of credit, including the *Yoskovich Funeral Home*.
3. **Customer**. A "customer" means a person or business entity that has an account with the *Yoskovich Funeral Home*.
4. **Identifying Information**. "Identifying information" means 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 or unique electronic identification number.

5. Identity Theft. "Identity Theft" means fraud committed using the identifying information of another person.

6. Red Flag. A "Red Flag" means a pattern, practice, or specific activity that indicates the possible existence of Identity Theft.

II. IDENTIFICATION OF RED FLAGS

In order to identify relevant Red Flags, the *Yoskovich Funeral Home* shall review and consider the types of accounts that it offers and maintains, the methods it provides to open accounts, the methods it provides to access its accounts, and its previous experiences with Identity Theft. The *Yoskovich Funeral Home* identifies the following Red Flags, in each of the listed categories:

A. Notifications and Warnings From Credit Reporting Agencies

Red Flags

1. Report of fraud accompanying a credit report;
2. Notice or report from a credit agency of a credit freeze on a customer or applicant;
3. Notice or report from a credit agency of an active duty alert for an applicant; and
4. Indication from a credit report of activity that is inconsistent with a customer's usual pattern or activity.

B. Suspicious Documents

Red Flags

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

C. Suspicious Personal Identifying Information

Red Flags

1. Identifying information presented that is inconsistent with other information the customer provides (such as inconsistent birth dates);
2. Identifying information presented that is inconsistent with other sources of information (for instance, an address not matching an address on a driver's license);
3. Identifying information presented that is the same as information shown on other applications that were found to be fraudulent;
4. Identifying information presented that is consistent with fraudulent activity (such as an invalid phone number or fictitious billing address);
5. Social security number presented that is the same as one given by another customer;
6. An address or phone number presented that is the same as that of another person;
7. Failing 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

8. Identifying information which is not consistent with the information that is on file for the customer.

D. Suspicious Account Activity or Unusual Use of Account

Red Flags

1. Change of address for an account followed by a request to change the account holder's name;
2. Payments stop on an otherwise consistently up-to-date account;
3. Account used in a way that is not consistent with prior use (such as very high activity);
4. Mail sent to the account holder is repeatedly returned as undeliverable;
5. Notice to the *Yoskovich Funeral Home* that a customer is not receiving mail sent by the *Yoskovich Funeral Home*;
6. Notice to the *Yoskovich Funeral Home* that an account has unauthorized activity;
7. Breach in the *Yoskovich Funeral Home*'s computer system security; and
8. Unauthorized access to or use of customer account information.

E. Alerts from Others

Red Flag

1. Notice to the *Yoskovich Funeral Home* from a customer, a victim of identity theft, a law enforcement authority or other person that it has opened or is maintaining a fraudulent account for a person engaged in Identity Theft.

III. DETECTING RED FLAGS

A. New Accounts

In order to detect any of the Red Flags identified above associated with the opening of a new account, *Yoskovich Funeral Home* personnel will take the following steps to obtain and verify the identity of the person opening the account:

Detect Red Flags

1. 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;
2. Verify the customer's identity (for instance, review a driver's license or other identification card); and
3. Independently contact the customer.

B. Existing Accounts

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

Detect Red Flags

1. Verify the identification of customers if they request information (in person, via telephone, via facsimile, via email);
2. Verify the validity of requests to change billing addresses; and
3. Verify changes in banking information given for billing and payment purposes.

IV. PREVENTING AND MITIGATING IDENTITY THEFT

In the event *Yoskovich Funeral Home* personnel detect 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:

Prevent and Mitigate Identity Theft

1. Monitor an account for evidence of Identity Theft;
2. Contact the customer with the account;
3. Change any passwords or other security codes and devices that permit access to an account;
4. Not open a new account;
5. Close an existing account;
6. Reopen an account with a new number;
7. Not attempt to collect payment on an account;
8. Notify the Program Administrator for determination of the appropriate step(s) to take;
9. Notify law enforcement; or
10. Determine that no response is warranted under the particular circumstances.

Protect Customer Identifying Information

In order to further prevent the likelihood of Identity Theft occurring with respect to *Yoskovich Funeral Home* accounts, the *Yoskovich Funeral Home* shall take the following steps with respect to its internal operating procedures to protect customer identifying information:

1. Secure the *Yoskovich Funeral Home* website but provide clear notice that the website is not secure;
2. Undertake complete and secure destruction of paper documents and computer files containing customer information;
3. Make office computers password protected and provide that computer screens lock after a set period of time;
4. Keep offices clear of papers containing customer identifying information;
5. Maintain computer virus protection up to date; and
6. Require and keep only the kinds of customer information that are necessary for *Yoskovich Funeral Home* purposes.

V. PROGRAM UPDATES

The Program will be periodically reviewed and updated to reflect changes in risks to customers and to the safety and soundness of the *Yoskovich Funeral Home* from Identity Theft. The Program Administrator shall at least annually consider the *Yoskovich Funeral Home's* experiences with: Identity Theft; changes in Identity Theft methods; changes in Identity Theft detection and prevention methods; changes in types of accounts the *Yoskovich Funeral Home* maintains; and changes in the *Yoskovich Funeral Home's* business arrangements with other entities and service providers. After considering these factors, the Program Administrator shall determine whether changes to the Program, including the listing of Red Flags, are warranted. If warranted, the Program Administrator shall update and implement the revised Program.

VI. PROGRAM ADMINISTRATION

A. Oversight

The Program Administrator shall be responsible for developing, implementing and updating the Program. The program Administrator for the *Yoskovich Funeral Home* is Martin J. Yoskovich, Owner & Funeral Director.

The Program Administrator shall be responsible for: Program administration; appropriate training of *Yoskovich Funeral Home* staff on the Program; reviewing any reports regarding the detection of Red Flags; the steps for preventing and mitigating Identity Theft; determining which steps of prevention and mitigation should be taken in particular circumstances; and considering periodic changes to the Program.

B. Staff Training and Reports

Yoskovich Funeral Home staff shall be trained either by or under the direction of the Program Administrator in the detection of Red Flags, and the responsive steps to be taken when a Red Flag is detected. The *Yoskovich Funeral Home* shall provide no less than annual training or upon any new employee hire. *Yoskovich Funeral Home* staff shall provide reports to the Program Administrator on incidents of Identity Theft, the *Yoskovich Funeral Home's* compliance with the Program and the effectiveness of the Program.

C. Service Provider Arrangements

In the event the *Yoskovich Funeral Home* engages a service provider, including but not limited to finance and insurance companies, to perform an activity in connection with an account, the *Yoskovich Funeral Home* shall take the following steps to require that the service provider performs its activity in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of Identity Theft.

1. Require that service providers acknowledge receipt and review of the Program and agree to perform its activities with respect to Yoskovich Funeral Home accounts in compliance with the terms and conditions of the Program and with all instructions and directions issued by the Program Administrator relative to the Program; or
2. Require that service providers acknowledge receipt and review of the Program and agree to perform its activities with respect to the Yoskovich Funeral Home accounts in compliance with the terms and conditions of the service provider's identity theft prevention program and will take appropriate action to prevent and mitigate identity theft; and that the service providers agree to report promptly to the Yoskovich Funeral Home in writing if the service provider in connection with a Yoskovich Funeral Home account detects an incident of actual or attempted identity theft or is unable to resolve one or more Red Flags that the service provider detects in connection with an account.