TRUST MANAGEMENT NETWORK
IDENTITY THEFT RED FLAGS POLICY

GENERAL STATEMENT

Trust Management Network ("TMN") is committed to protecting its client customer base from unauthorized activity and identity theft. Identity theft may be defined as a fraud attempted or committed using identifying information of another person without authority. In an effort to prevent identity theft, this Policy compliments TMN's existing Data Breach Notification Policy. The objectives of this Policy is to identify our program for detecting red flags, preventing identify theft and mitigating risks to promote compliance with federal regulations. A "red flag" is defined as a pattern, practice or specific activity that indicates the possible existence of identity theft.[1] This Policy is considered appropriate given the activity and services TMN provides to its clients and the limited interaction that TMN has with client customers. This Identify Theft (Red Flags or Program) Program includes the following:

- A written Program or Policy
- A periodic report to the Board or members of Senior Management as appropriate
- Oversight Responsibility
- Red Flag detection, prevention, and mitigating controls and response actions

A well designed identity theft prevention program will help the TMN and its clients to avoid fraud losses and protect customers. This program will also protect financial soundness and reputational risk. Our goal is to reasonably determine foreseeable internal and external threats and to ensure that controls are in place to minimize threats and probability of occurrence.

ACCOUNTS COVERED

The identity theft prevention regulation generally covers most consumer accounts used primarily for personal, family, or household purposes. While client customer accounts can be held by both individuals and entities, this policy serves to cover accounts held by individuals. Covered accounts generally involve accounts that have the ability to permit multiple payments or transactions maintained by a client for which there is a reasonably foreseeable risk to the consumer. While TMN does not deal directly with client trust customers and conducts transactions only when authorized by a client, it is the client's responsibility to ensure that its customer's identity is verified and that transactions are authenticated prior to submission to TMN. In an effort to provide mitigating controls to prevent identify theft, TMN has identified red flags that serve to identify and prevent identity theft based upon the services offered to its clients.

[1] Identity Theft is a fraud committed or attempted using the identify information of another person without authorization. Identifying information includes any name or number used alone or in conjunction with other information specific to a person including: name, SSN, date of birth, driver's license or ID, passport number, tax ID, unique biometric data or other physical representation, unique electronic routing, address or identification number, or telecommunicating identifying information or access device or card.

RED FLAGS DETECTION AND RESPONSIBILITY

The following are considered red flags that TMN may identity to detect a pattern or practice which could be the result of identity theft:

- Documentation provided to TMN to open an account that appears to be altered or not properly authorized by the client
- Information provided to TMN that is associated with known fraudulent activity
- A change of address request that is not properly authorized or appears to be fictitious such as a mail drop or prison
- A material change in transaction patterns such as an unexplained and noticeable increase in the number of withdrawals or distributions on an account that is inconsistent with the accounts normal history
- Accounts that have been inactive for a reasonable lengthy period are suddenly experiencing unexplained withdrawals or distributions

TMN personnel are responsible for being aware of red flag characteristics and responding accordingly. Should a red flag event be identified by TMN, the occurrence must be brought to the attention of a senior management officer of TMN. TMN senior management will evaluate the red flag information and contact the client to discuss the transaction(s) and to determine that the transaction is properly authorized. TMN will not have any direct contact with client customers.

EFFORTS TO PREVENT OF IDENTITY THEFT

TMN does not share client customer information so risk from external threats is reduced. Client Control Considerations, outlined in TMN's SSAE 16 report, gives information regarding each client's responsibility to ensure that client controls over transactions and data submissions to TMN are accurate. This means that each client is responsible for ensuring that customer transactions are authentic and that such requests are not the result of identity theft. TMN does not have fiduciary or any other contractual responsibility over administration of client accounts and does not collect or have access to information obtained by the client to authenticate client customers. Additionally, customers do not access TMN's systems directly but rather sign-in directly to the SunGard trust accounting platform know as PAL that is maintained on each client's website. Given the controls that have been put in place to ensure accurate and authenticated transactions are sent to TMN, efforts to prevent identify theft are considered appropriate.

RISK MITIGATION

Given TMN's very limited interactions with client customers and the internal control authorization structure TMN has in place to ensure transactions are properly authorized by the client, risks associated with identify theft are considered mitigated and low. Adequate policies and processes are in place and appear effective in detecting, preventing and mitigating risk. Capable management oversight exists. Training, through access to this Policy and discussions regarding identity theft and red flags during periodic staff meetings, is appropriate.