TRUST MANAGEMENT NETWORK
DATA BREACH NOTIFICATION POLICY

GENERAL STATEMENT

Trust Management Network ("TMN") has an affirmative and continuing obligation to respect the privacy of its Client's customers. TMN protects the security and confidentiality of its Client customer nonpublic personal information through a combination of a Privacy Policy and a Code of Ethics Policy for its employees, as well as the contractual terms contained in each Client's Data Processing and Custodial Services Agreement ("Agreement"), which outlines the terms of services being offered by TMN.

This data breach notification policy is to provide a framework from which TMN will respond to its discovery or notification from an outside third party vendor with which TMN contracts for services that a Client's customer nonpublic personal information has been compromised.

The definition of a data breach for purposes of this policy means the unauthorized acquisition of computerized data that compromises the security, confidentiality, or the integrity of personal information maintained by TMN.

POLICY OBJECTIVES

The purpose of this policy is to recognize the importance of information security and to realize that a data breach may still occur and therefore to establish the basis for how TMN will address such a data breach should one occur notwithstanding the reasonable efforts already in place that would prevent such a data breach.

POLICY

In the event TMN discovers through its internal information monitoring systems or from an external source that a Client customer's nonpublic personal information has been breached, then TMN will promptly notify the person(s) designated in the Agreement that a data breach has occurred, when it was reported, the extent of the data breach as known to TMN and what action plans have been implemented by TMN or its third party vendor to secure and control the data breach.

TMN has a contractual arrangement with SunGard Business Systems, LLC ("SunGard") whereby SunGard will promptly contact TMN when it, i.e. SunGard, determines that the user information, i.e. Client customer nonpublic personal information, has been acquired by an unauthorized person, unless SunGard is restricted from doing so by applicable law or law enforcement officials. In the event SunGard is prohibited from contacting TMN about an unauthorized access event by law enforcement officials, SunGard will contact TMN and advise it of said unauthorized access event promptly upon receiving permission to do so from said law enforcement officials.