

Method and system protecting against identity theft or replication abuse

Abstract

A system detecting and protecting against identity theft by abusing a computer users ID and password or protecting a user against identity replication through parallel user session via a second authentication level using a second channel, a one-time-passcode and user contextual location information. When accessing networks, computer systems or programs, the said networks, computer systems or programs will validate user ID and password and collect contextual information about the user, the device, the used network etc. Once validated, a message is send by a second means that may be a cell phone SMS network or an instant message, said message containing a real-time session-specific one-time passcode. The session specific code and the collected information provides information enabling the user to detect a compromised identity through a mismatch between presented information and the information representing the user and the passcode protects against fraudulent access.

Fig. 1