Direct Authentication System and Method via Trusted Authenticators

U.S. Patent Application of

Nader Asghari-Kamrani

and

Kamran Asghari-Kamrani

Direct Authentication System and Method

via Trusted Authenticators

This application is a continuation-in-part of U.S. Patent Application No. 09/940,635 filed August 31, 2001, and claims priority to U.S. Provisional Application No. 60/650,137 filed February 7, 2005.

BACKGROUND OF THE INVENTION

1. FIELD OF THE INVENTION

The present invention generally relates to a direct authentication system and method, more particularly, to a new two-factor authentication method used by a business to authenticate its customers' identity utilizing trusted-authenticators.

2. DESCRIPTION OF THE RELATED ART

Fraud and Identity theft, the taking of a person's identity for the purpose of committing a criminal act, is a growing national concern, both in terms of its affect on its victims, and its potential national security implications. Checking account fraud costs US banks USD 698 million in 2002, according to the American

Bankers' Association, while those perpetrating the fraud attempted to take USD 4.3 billion in total. Identity theft costs financial institutions USD 47.6 billion in 2002-2003. A report issued in September 2003 by the Federal Trade Commission estimates that almost 10 million Americans were victims of some type of identity theft within the previous year. Especially unnerving are the numerous accounts of the ordeals that victims endure as they attempt to deal with the results of this crime. They are assumed to be responsible for the debts incurred by the thief until they can demonstrate that they have been victims of fraud. They are targeted by collection agencies trying to collect on debts generated by thieves who open new accounts in their name. They have to deal with damaging information placed in their credit files as a result of the imposter's actions. It's well known how this can happen. Fraudulent charges may be posted to someone's checking account if the thief knows the account number and banks routing number. Identity thieves can "take over" an existing account and withdraw money, as well as change other account information such as mailing address, if the thief knows a few pieces of sensitive personal information, especially the account holder's Social Security Number (SSN). Perhaps worst of all, a thief can easily open a new account in someone else's name by completing an application for a new credit account, using the victim's name and SSN, but with a different address. The credit grantor, whether it be a retailer offering instant credit accounts via their website, a telecommunications company offering a new cell phone account, a bank offering a credit card, or an auto dealership offering a new car loan, uses the information provided by the thief to obtain a credit report on the person named in the account application. If the report indicates that the person named in the application is a good credit risk, a new account will likely be opened in the victim's name. But the victim never knows about the late and unpaid bills, until his credit is ruined.

Online Fraud happens because online businesses such as retailers assume that the person shopping online is the same person whose personal or financial information are given. Identity theft happens because creditors assume that the person filling the application is the same person whose name and personal information are used in the application, unless there is clear evidence to the contrary. A business "authenticates" a customer by matching personal and financial information provided, such as name, SSN, birth date, etc., with information contained in third party databases (indirect authentication). If there is a match on at least a few items of information, it is assumed that the person is the same person who he says he is. This assumption itself is a direct result of a belief that sensitive personal and financial information can be kept secret and out of the hands of thieves. Yet the widespread incidence of fraud and identity theft, as detailed by the personal stories of its many victims, clearly demonstrates that this notion is false. A recent paper by Prof. Daniel Solove ("Identity Theft, Privacy, and the Architecture of Vulnerability", Hastings Law Journal, Vol 54, N o. 4 (2003), page 1251) of the Seton Hall Law School aptly points out that "*The identity thief's ability to so easily access and use our personal and financial data stems from an architecture that does not provide adequate security to our personal and financial information and that does not afford us with a sufficient degree of participation in the collection, dissemination, and use of that information."* He further goes on to say "*The problem, however, runs deeper than the public disclosure of Social Security Numbers (SSN), personal and financial information. The problem stems not only from the government's creation of a de facto identifier and lax protection of it, but also from the private sector's inadequate security measures in handling personal information*". "*Further, identity thieves can obtain personal and financial information simply by paying a small*

fee to various database companies and obtaining a detailed dossier about their victims." There's only a certain amount that an individual can do to prevent sensitive information from getting into the wrong hands, such as keeping a tight grip on one's purse or wallet. Beyond that, the information is easily available to a thief in numerous other ways. It may be available through certain public records. It can be purchased from publicly available databases for a nominal fee. It can be copied from medical claims forms lying around in a doctor's office. Other methods include breaking into various commercial databases containing sensitive information about business's customers, many times with the help of an insider. As long as the authentication of new credit applications is based upon knowledge of a few items of personal information that are supposed to be confidential, the only way to truly prevent this type of identity theft is to keep one's personal information out of the hands of thieves, an impossible task. This is also true in the case of identity theft involving account takeovers, in which the thief uses knowledge of personal information about the victim to obtain information needed to take over someone's existing account.

There have been many attempts to solve above issues and concerns. One being the recent paper by Prof. Lynn LoPucki of the UCLA School of Law (www.ssrn.com/abstract=263213). The paper addresses many of these concerns, and suggests an approach to the identity theft problem that addresses the fundamental flaws in the process. This approach does not depend on keeping personal information secret, asking out-of-wallet questions, or computing fraud scores based on historical data and analytical fraud models. LoPucki's approach, which he calls the Public Identity System (PIDS), would establish a voluntary list of people concerned about identity theft, and who consent to be directly contacted for verification when someone applies for credit in their name.

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.