

**Comments on
National Strategy for Trusted Identities in Cyberspace
July, 2010**

Bob Pinheiro
Robert Pinheiro Consulting LLC

One of the motivations behind NSTIC is to protect consumers against identity theft and other types of online identity-related fraud. From the consumer protection point of view, an identity ecosystem could support this goal for those consumers who choose to participate, provided that it supports appropriate privacy protections as well.

With this in mind, I have the following suggestions:

1. NSTIC should devise strong incentives to engender support and deployment of the identity ecosystem by the financial services community.

Much identity-related fraud involves financial transactions. It's difficult to imagine that an identity ecosystem can be truly effective in helping prevent identity fraud unless financial institutions participate. Yet at the consumer (and small business) level, online authentication for financial transactions is often still based on passwords, backed up by weak and cumbersome self-selected challenge questions. Incentives are needed to encourage banks and other financial services providers (e.g., mutual fund companies, brokerages, payment services, etc.) to participate in the identity ecosystem. Financial institutions could offer, on an opt-in basis, electronic credentials to consumers that can be used for strong authentication in online financial transactions. Participation might also involve creation of a new organization or consortium, run by the financial community, to provide these credentials to consumers who want them. By means of a trust framework adopted by this consortium, financial institutions that are consortium members could trust credentials and assertions issued by other members of the consortium. By sharing costs for strong credentials among members of such a consortium, it may become more economical for financial institutions to provide strong authentication for consumers and small businesses.

2. NSTIC should recognize that consumer transactions requiring strong authentication may not always require an identity assertion or claim issued by an Identity Provider.

Certain categories of online transactions may result in harm to the consumer if others are able to successfully use the consumer's personally identifiable information to impersonate him/her. Such categories would include: (a) transactions that result in the establishment of a new high value relationship such as a credit account (credit card, loan, etc); (b) transactions that provide access to sensitive personal information such as health records, bank account balances, or a free annual credit report; (c) transactions that

involve moving money out of financial accounts; (d) transactions in which an online payment is made using bank account or credit card information.

Assuming that strong authentication enabled by the identity ecosystem can be used to help prevent fraud in each of these categories of transactions, the first category (a) would most likely require that an Identity Provider return an assertion/claim to a Service Provider / Relying Party containing information that establishes the identity of a specific individual. The second category (b) would require such assertions/claims if the consumer is unknown to the Service Provider / Relying Party, or has not otherwise established a previous relationship with the Service Provider / Relying Party. Once such a relationship is established, it should be sufficient for the consumer to present to the Service Provider / Relying Party some sort of token that employs strong (multifactor) authentication to demonstrate that he/she is the “owner” of the previously-established relationship or online resource. Categories (c) and (d) assume that an existing financial or payment account exists, so again it should be sufficient to present an appropriate strong authentication token to transact a payment or move money out of an existing account.

In other words, an identity assertion/claim containing personally identifiable information (ie, name, address, birthdate, etc.) from an Identity Provider is necessary in order to initially establish the identity of someone seeking a new relationship or account with a Service Provider / Relying Party. Once the relationship is established, it may be sufficient for a credential or token issued by the Identity Provider to be used locally by the Service Provider to authenticate the consumer (or the specific transaction) without an assertion/claim from an Identity Provider each time such authentication is required. This may remove potential concerns by Service Providers that they must depend on the availability of a third party Identity Provider in order for their customers to be able to conduct business with the Service Provider, or that they may have to pay an Identity Provider something for each authentication.

As an example, an X.509 certificate issued to a consumer could be used to establish the identity of a consumer with a Service Provider / Relying Party. Once the consumer authenticates to the issuing Identity Provider using the consumer’s private key, the Identity Provider then issues a trusted assertion / claim to the Service Provider / Relying Party that contains sufficient information to establish the consumer’s identity. Once identity is established, the certificate and its associated public key could be bound to the consumer’s identity by the Service Provider, and the returning consumer could directly authenticate to the Service Provider using an appropriate authentication protocol that demonstrates control and possession of the private key.

- 3. While strong incentives should exist for the adoption and use of high assurance electronic credentials in high value transactions, NSTIC should consider measures to create strong dis-incentives for the use of high assurance credentials to establish a person’s identity in low-value transactions.**

It's not difficult to imagine that if high assurance electronic credentials ever become widely used by consumers for high-value transactions, some Service Providers may decide to demand such credentials for high assurance identification even for low value transactions. NSTIC should articulate potential measures to discourage the use of high assurance credentials to establish one's identity in low value transactions where knowledge of identity isn't necessary. For instance, high assurance assertions that convey identity information about a consumer may have a "cost" that providers of low value services might not be willing to pay.

4. Potential Role for Consumer Reporting Agencies / Credit Bureaus in NSTIC

The identity ecosystem is voluntary, and Service Providers / Relying Parties are under no obligation to participate. However, the ability of an identity ecosystem to help prevent identity fraud depends on widespread deployment and adoption. In the meantime, what's to stop a thief who obtains someone's personal information from using it to open a new credit card, for example?

Prior to establishment of certain kinds of high-value accounts and relationships, Service Providers often use Consumer Reporting Agencies (also known as credit bureaus) to determine the creditworthiness of consumers. This involves collecting sufficient personally identifiable information from a consumer, and sending it to the credit bureau where it is matched to a record the credit bureau may maintain about the consumer.

If that consumer has chosen to be a participant in the identity ecosystem, and is in possession of credentials that can authenticate his/her identity, perhaps the credit bureau, on making a match, can act as a go-between to alert the consumer that someone is attempting to use his/her information to establish a high value relationship with some particular Service Provider. This would require that credit bureaus allow such individuals to register their status as identity ecosystem participants. The potential actions that such a consumer could then take is left for future discussion.

Of course, credit bureaus can also act as Identity Providers in the identity ecosystem.

5. The Federal Trade Commission should have a prominent role in the identity ecosystem.

The Federal Trade Commission is the nation's consumer protection agency. The FTC is involved in other government efforts to prevent identity theft. These include acting as the enforcement agency for the Fair Credit Reporting Act, and promulgating the so-called "Red Flag Rules" for identity theft prevention. The FTC should, at minimum, take an active role in helping to educate the public and the business world about the identity ecosystem.