

# How Can NSTIC Help Prevent Identity Theft?

Bob Pinheiro  
Robert Pinheiro Consulting LLC  
bob@bobpinheiro.com

On April 15, 2011 the US government released the National Strategy for Trusted Identities in Cyberspace (NSTIC), which proposes that the private sector lead the development and implementation of an “identity ecosystem” as a platform for establishing better trust among individuals and other entities engaged in online transactions. More specifically, NSTIC “focuses on ways to establish and maintain trusted digital identities, which are critical for improving the security of online transactions.”

One of the motivations for NSTIC is to help protect consumers against identity theft, which can be defined as the impersonation of specific individuals by fraudsters for the purpose of obtaining high value services using the consumer’s identity. Identity theft causes consumers to be harmed when:

- New credit accounts such as loans, credit cards, charge cards, cell phone accounts, etc., are established by a fraudster using the consumer’s identity information. Not only will the consumer be asked to pay for purchases they didn’t make, but the consumer’s credit report and score are likely to be damaged when fraudsters run up charges on these accounts, and then don’t pay.
- Medical services are provided to a fraudster, who assumes someone else’s identity to obtain these services. Not only will the identity theft victim be stuck with the bill for these services, but the victim’s own medical history can be contaminated by information about treatment provided to the fraudster.
- Fraudsters are able to “hijack” an individual’s financial accounts by stealing login credentials such as passwords and challenge questions. Fraudsters can then move money out of these accounts in various ways.
- Fraudsters obtain merchandise and other services without paying, by using stolen credit card information, or stolen bank account information, to bill the charges to the victim’s credit card, or to setup payment directly from a victim’s bank account. In both cases, it is up to the victim to notice the bogus credit card charges or debits from their bank account, and challenge them in a timely manner.
- A fraudster obtains employment using someone else’s social security number. This can cause the IRS to believe that the identity theft victim earned more wages than the victim actually reported.

All of these examples point to the same underlying problem: a failure of the providers of these services to adequately authenticate the identity or authorization status of those to whom it is providing these services.

## Do Trust Frameworks Provide Assurance Against Impersonation?

One of the key components of an identity ecosystem such as envisioned by NSTIC is a *trust framework*, whose purpose is to define the rules that the various actors within a *trust community* must comply with, so that various degrees of assurance regarding identity-related claims within that community may be achieved. Trust frameworks that are currently defined tend to be service-provider centric in that their main focus is to enable service providers to have a certain level of assurance about the identity of someone seeking a service. In order for service providers to have this assurance, they will likely obtain verified personal information about such individuals. To better protect the privacy of the consumer's information, it's been proposed that an additional "privacy framework" be specified to help ensure that entities within the identity ecosystem that maintain and store personal information about individuals will treat and manage that information according to certain privacy constraints.

While these privacy constraints provide some assurance to consumers that their personal information will be protected, there's another user-centric question that has largely gone unaddressed. Do consumers within a trust community governed by some trust framework have any assurance against being impersonated within that community? And if not, should they?

[Note that although we are concerned here about identity theft as it affects consumers, similar concerns exist regarding businesses as well. For example, a small business may have its bank account cleaned out by thieves if various kinds of information or login credentials are compromised.]

## Assurance Against Impersonation Is Different Than Protection of Personal Information

An individual participates in a trust community if that individual's identity<sup>1</sup> has been verified by an identity proofing process (at some assurance level), as specified by the governing trust framework. As a result of the proofing process, the individual is issued a corresponding credential that is trusted by service providers / relying parties within the community.

The issue of impersonation that is addressed here is not a concern about an imposter being able to impersonate someone else during the credential-issuing process. We'll assume that the trust framework's identity proofing and credential issuance criteria, as well as their actual implementation, provide sufficient assurance against this happening.

This is also different from the privacy issue. The question of whether an individual is protected against impersonation within a trust community does not strictly depend on how their personal information is handled by service providers or identity providers.

---

<sup>1</sup> We'll define "identity" as some collection of attributes pertaining to an individual that are meaningful to service providers in some trust community, as they decide whether to provide their service to the individual.

Assuming that impersonation can be prevented during the credential-issuing process by means of a sufficiently rigorous identity proofing procedure, a consumer can still be impersonated if service providers are willing extend services to someone who is not authenticated at the appropriate assurance level. Of more specific concern to the individual consumer is whether a service provider is willing and able to reject false claims to the consumer's identity that are made by a would-be imposter.

### Participation in Trust Communities is Voluntary

If every service provider / relying party chooses to require everyone seeking a service from it to submit a trusted credential (at an appropriate assurance level) for identity authentication, consumers would have some degree of assurance against being impersonated.

But NSTIC contains no requirement that service providers authenticate everyone seeking a service from it, and it's doubtful whether service providers would even find such a requirement to be desirable. Indeed, NSTIC is very clear that participation in the identity ecosystem will be voluntary. And although identity fraud may be reduced if service providers choose to participate in the identity ecosystem and require authentication at the appropriate assurance level for enrolling in high value services, such a requirement would essentially limit the customers of those service providers to individuals also participating in the same trust community<sup>2</sup>.

If service providers offering high value services do not require adequate authentication of everyone seeking those services, then identity thieves seeking to impersonate others can still be successful. Yet it is not unreasonable for consumers who voluntarily choose to participate in a trust community, and who have obtained the appropriate credentials, to expect immunity from impersonation within that community (at some assurance level). Is there any way to provide such consumers with assurance against impersonation when there is no requirement for anyone to participate in the identity ecosystem?

### How Can Assurance Against Impersonation Be Achieved in a Voluntary Identity Ecosystem?

Even if a service provider does not participate in a NSTIC-compliant trust community, or does participate but does not require authentication of everyone seeking a service, consumers may still be able to have some assurance against impersonation, in certain circumstances. One possibility for achieving such assurance relies on the fact that almost all consumers who have engaged in financial transactions of one sort or another are likely to have a credit history and score maintained by one or more of the consumer reporting agencies (i.e., the "credit bureaus" Experian, Trans Union, and Equifax). Providers of high value services such as credit cards, cell phone accounts, and other credit-dependent services often rely on knowledge of a consumer's credit score in order to decide whether to enroll individuals in such services. Without such a credit score to assess the

---

<sup>2</sup> Or possibly other interoperable trust communities that the service provider / relying party determines to offer comparable levels of assurance.

creditworthiness of applicants for high value services, many service providers will not enroll a new customer in the service.

As a tool against identity theft, credit bureaus offer consumers the ability to “freeze” their credit reports, so that a request by a service provider for a credit report / score on an individual with a “frozen” credit report will not be granted by the credit bureau unless the consumer first “unfreezes” his/her credit report. However, the credit freezing and unfreezing process is costly, time consuming, and cumbersome for the consumer.

One possible way to provide consumers who participate in the identity ecosystem, and who possess NSTIC-compliant credentials, with some level of assurance against impersonation would depend on the credit bureaus allowing those consumers to register their credentials with the credit bureau<sup>3</sup>. When a request for the credit score of any such individual is received by the credit bureau from a service provider (as part of the process to enroll the individual in a high value service), the credit bureau could voluntarily agree not to release any credit information to the service provider unless it can first authenticate (by means of these credentials) that the person whose credit score is being requested is the same person who is seeking to enroll in the service. If such authentication can not be obtained by the credit bureau, that fact could be transmitted to the service provider, alerting it that the individual seeking to enroll in the high value service may be an imposter.

This approach may be viable only in certain situations, such as when the identity theft involves establishing a new credit-bearing account using the victim’s identity, and it requires the cooperation of credit bureaus. But it serves as an example of how an identity ecosystem conformant with NSTIC principles may help to prevent identity theft even when service providers may not be ecosystem participants themselves, and before widespread adoption of NSTIC by service providers.

The author is interested in receiving any comments or suggestions you may have about this approach to identity theft prevention.

---

<sup>3</sup> Credit bureaus themselves may be identity providers within the identity ecosystem, and may issue such credentials directly to consumers.