

Map The Gaps Position Paper
March 18-19, 2010

Bob Pinheiro
Robert Pinheiro Consulting LLC
& Chair, Kantara Consumer Identity Work Group

bp@bobpinheiro.com

Businesses that provide identity-dependent, high value services to consumers have certain legal obligations to their customers. Such obligations may involve protecting the customer's personal information, protecting funds on deposit with the business, etc. The legal issue I want to raise is whether any duty-of-care also exists (or should exist) to the person whose identity is used when such high value services are established, whether or not that person is the one actually seeking the service.

There are many situations in which someone must identify himself/herself to a service provider in order to obtain some identity-dependent service. Such a service could be a new credit card, or new car loan, or even a medical procedure. Depending upon the type of service provided, serious harm might befall someone whose identity is misappropriated or "stolen" by a fraudster in order to obtain the service. In the case of opening a new credit card, the identity theft victim could suffer at least two types of harm. The victim's credit history could be damaged if the fraudster opens the account and then doesn't pay the bills. The identity theft victim could also be harmed by intimidating calls from collection agencies seeking to collect the money actually owed by the identity thief, or harmed by a legal judgment for the amount due. In the case of medical identity theft, the victim's medical history can be contaminated by information pertaining to treatment provided to an imposter who used the victim's identity to obtain the treatment.

The legal question is whether entities that provide certain kinds of high value, identity-dependent services bear any legal duty-of-care to the person whose identity is used to obtain the service, whether or not that person is actually the one seeking the service. It's not clear whether such a duty exists. The basis for this duty-of-care would be that an action taken by a service provider on behalf of an identity thief could cause harm to the person whose identity was "stolen." The obligation of the service provider would be to take reasonable measures to ensure that the identity claimed by a person seeking such a service is actually that person's true identity. This seems to be a bit different than a desire on the part of the service provider to know the identity of the person seeking the service. In the former case, a duty-of-care may exist to protect individuals against the harms resulting from identity theft. In the latter case, the benefit is mainly to the service provider.

This type of obligation also seems to be different than what the new Red Flag Rules require in situations where the service is a credit account such as a loan or credit card.

The Red Flag Rules require that a creditor have an “identity theft prevention program” in place that specifies “red flags” whose presence may indicate that identity theft is occurring. It further requires an action plan for reacting to the red flags. The duty-of-care suggested here would exist independent of whether a service provider notices anything suspicious.....there would always be some requirement to take a reasonable action to determine whether the identity being used to obtain certain kinds of high value services actually belongs to the person seeking the service.

In days past it may have been cumbersome and expensive for service providers to verify the identities of those who seek high value services. But the emergence of federated “identity networks” of relying parties (RPs) and credential service providers (CSPs), which presumably will provide increasing numbers of individuals with high assurance credentials, may make it more feasible for RPs to determine whether a claim of identity is legitimate.

For example, suppose my identity has been “proofed” by some CSP that has issued me high assurance credentials. If CSPs and RPs are networked in some way to form an identity network, it might become feasible for the RP to query this network to determine whether there is a CSP that “knows” me. This would be important if I, or someone else claiming my identity, were trying to obtain a high value service. If so, the identity network is presumed able to somehow initiate contact with me, and request that I authenticate to my CSP in order to confirm (or deny) that the person claiming my identity is actually me. The CSP would then provide an assertion back to the RP with this information.

It’s likely that an identity thief who is claiming someone else’s identity will make the claim simply on the basis of knowledge of personally identifiable information (PII). This is because it’s unlikely that any service providers / RPs will require that potential customers possess trusted, high assurance credentials prior to obtaining the service....at least not until the use of such credentials becomes widespread. So the identity network would need to match this PII to an identity known to some trusted CSP. This, however, requires that identities recorded at CSPs be defined in terms of a set of identifiers (such as name, address, birthdate, social security number or other government id number, etc.) that can be matched against the PII provided by the imposter. This has implications for the identity proofing process, to the extent that the proofing process needs to verify commonly used identifiers that would likely be included in stolen PII.