Consumer Identity WG - Proposed Charter Revisions (September 28, 2010)

(2) PURPOSE: *Please provide a clear statement of purpose and justification why the WG is necessary.*

Online identity fraud results from the misuse of personally identifying information such as names, Social Security Numbers, and birthdates, as well as misuse of shared secrets such as passwords, credit card information, answers to "challenge questions", mother's maiden name, etc. Misuse of this PII enables fraudsters to impersonate individual consumers online because identity-related claims are often based on nothing more than knowledge of this information. Identity fraud has an obvious negative impact on consumers, who may experience damaged credit scores, drained bank accounts, fraudulent credit card charges and other bills resulting from unauthorized purchases, falsified medical histories, privacy breaches of sensitive medical records and information, etc. The negative impact on businesses that provide identity-related products or services includes damage to their operations, reputations, and bottom line, as well as loss of consumer trust that is difficult and costly to regain.

The purpose of the Consumer Identity WG is to foster the development of a consumer-friendly, privacy-protecting, high assurance "identity layer" for the internet that enables consumers to fully exploit the potential of the internet without fear of identity theft. The WG addresses this goal by proposing technical and policy solutions that address current threats to privacy and identity, and socializes these solutions with appropriate parties to help foster their implementation.

(3) SCOPE: *Explain the scope and definition of the planned work.*

While a number of initiatives, frameworks, and technologies currently exist that can support the purpose of this WG, today there is no large-scale, practical way to verify online identity-related claims as they pertain to individual consumers. Initiatives, technologies, frameworks, etc. that currently contribute to this goal include the Liberty Alliance Web Services Framework, the Liberty Alliance Identity Assurance Framework, Initiative for Open Authentication (OATH), the US government's e-Authentication initiative, OpenID, Information Cards, public key infrastructures (PKI), knowledge-based authentication, and others.

In addition to acting as a general source of information and expertise on issues related to consumer identity and identity theft, the Consumer Identity WG seeks to propose solutions to the problem of online consumer identity assurance that

- facilitates trust of consumers by services providers
- facilitates trust of service providers by consumers
- reduces the amount of PII required to conduct sensitive transactions
- protects the privacy of consumers using high assurance identity solutions for conducting high-value online transactions

Specifically, the WG will create several Whitepapers, and possibly other Requirements or Recommendations, to describe how emerging identity technologies, protocols, frameworks, laws and regulations, etc., can be leveraged to: (a) enable businesses to know, with high confidence, the identities (or authorization status) of individual consumers with whom it engages in high-value online transactions, without jeopardizing the privacy of the consumer's personally identifiable information; and (b) enable individual consumers to prevent others from impersonating them in high-value, online transactions.

By championing the use of high assurance, privacy-protecting identity solutions geared to individual consumers, the WG seeks to help bring about an environment in which the value of stolen personal information as an enabler of online identity theft and other identity fraud is greatly reduced. Although the scope of the Consumer Identity WG is geared to high assurance identity solutions for consumers, the WG is not constrained to address only high assurance identity issues, but may also address lower assurance identity solutions for consumers, provided there is sufficient interest by WG participants.

(4) DRAFT TECHNICAL SPECIFICATIONS: *List Working Titles of draft Technical Specifications to be produced _(if any), projected completion dates, and the Standards Setting Organization(s) to which they will be submitted upon approval by the Membership.*

No draft Technical Specifications are planned.

(5) OTHER DRAFT RECOMMENDATIONS: *Other Draft Recommendations and projected completion dates for submission for All Member Ballot.*

The Consumer Identity WG will undertake the following activities, **provided sufficient resources are available:**

a) Using a number of sources (see Section 10) as background, together with new insights derived from participation and interaction with industry groups and other identity-related initiatives, **the WG will produce ~~at least one~~ up to three ~~Whitepaper~~ individual Kantara Initiative Recommendation(s) or CIWG Reports that together (1) reports on the current state of high assurance / strong authentication applications for consumers, and expands on the challenges and roadblocks that need to be overcome; (2) recommends specific functions or capabilities of an identity infrastructure needed to support high assurance consumer applications, where high assurance may relate to other types of claims in addition to identity; and (3) addresses feasibility issues and provides guidance for the widespread implementation and deployment ("rollout") of this identity infrastructure. ~~that defines the concept of an authentication network comprised of Identity Providers that verify consumer identities and issue "strong" identity credentials to the consumers whose identities it has verified, Service Providers / Relying Parties who trust and rely on identity services from these Identity Providers, and individual consumers in posssession of these credentials.~~** ~~The Whitepaper(s) will specifically~~

~~address the needs of individual consumers to control the use of their online identities for obtaining identity-dependent services from Service Providers, as well as the needs of Service Providers to establish trusted relationships with Identity Providers who are then able to authenticate identity-related claims made by legitimate consumers known to these Identity Providers.~~

b) Information Cards, in particular, may hold special promise as a basis for online consumer identity solutions because of their intuitive visual user interface as electronic "identity cards." Information Cards can help prevent identity fraud in at least two ways: managed Information Cards issued by trusted third party Identity Providers can provide verified identity claims on behalf of consumers, and self-issued Information Cards implementing cryptographic authentication protocols can be bound to existing online resources or accounts to provide authentication of returning authorized users. **The WG will (depending on interest and available resources) produce a ~~Whitepaper~~ Kantara Initiative Recommendation or CIWG Report proposing use cases or other guidance that demonstrate how technologies such as Information Cards, OpenID, U-Prove, etc., can be used to enable high assurance identity claims for high value consumer transactions. ~~and in particular managed Information Cards, can provide high assurance identity solutions for consumers that can help prevent identity theft.~~** ~~The Whitepaper may propose or evaluate ways in which an "identity assurance framework" can be applied to establish trust between Relying Parties who consume identity claims contained in secure electronic tokens, and the Identity Providers who issue managed Information Cards as well as the identity claims transmitted via secure tokens. The Whitepaper may also address the problem of incorporating consumer-friendly, multifactor authentication schemes into the Information Card paradigm, replacing passwords as the only mechanism by which consumers authenticate to their Selectors (ie, online "wallets" holding Information Cards) and/or Identity Providers.~~

c) Much identity theft occurs because identity claims made by providing personally identifiable information are often unverified. Unless all or most Service Providers / Relying Parties require rigorous identity verification prior to establishing high-value, identity-related services, it may still be possible for the identity of someone who has been issued "strong" credentials to have his/her identity "stolen." **The WG will (depending on interest and available resources) produce a ~~Whitepaper~~ Kantara Initiative Recommendation or CIWG Report that explores the ~~feasibility of enabling a Relying Party to discover trusted Identity Providers that can verify an identity claim made on the basis of PII, provided that the PII corresponds to some individual consumer whose identity has been previously verified by a trusted Identity Provider.~~ feasibility of enabling consumers to discover and block attempts by unauthorized persons to use consumer's personally identifying information (PII) to claim their identities for obtaining / accessing high value services.**

The **ability to complete these deliverables, including** timeframes for completion of these activities, is dependent on available resources. We generally expect to complete ~~at least one~~ **the deliverables** described in (a) above within ~~4 months – 8 months~~ **12 months** of **receiving commitment of resources to pursue this work.** ~~approval of this charter.~~

Completion of ~~Whitepapers~~ **deliverables** described in (b) and (c) will ~~follow,~~ **depend on interest and availability of resources.**

~~Upon completion of the Whitepapers deliverables described above, the WG may choose to issue additional Recommendations or Requirements for the deployment or use of the consumer identity solutions discussed in the Whitepapers.~~

(6) LEADERSHIP: *WG Chair and Editor(s) (if any) subject to confirmation by a vote of the WG Participants.*

Bob Pinheiro, Robert Pinheiro Consulting LLC, consumerid (at) bobpinheiro (dot) com

(7) AUDIENCE: *Anticipated audience or users of the work.*

Organizations geared to reducing online identity fraud, credit card companies and others involved with online payments, non-profit identity and privacy groups, vendors of authentication and identity services and technologies, government consumer groups (e.g., FTC), credit reporting agencies, think tanks involved with identity issues (ie, Center for Strategic and International Studies, Center for American Progress, National Research Council, Center for Applied Identity Management Research, etc.), other relevant industry consortia.

(8) DURATION: *Objective criteria for determining when the work of the WG has been completed (or a statement that the WG is intended to be a standing WG to address work that is expected to be ongoing).*

The Kantara Leadership Council charters the Consumer Identity Work Group for five years. It may be amended from time to time, with changes approved by the Leadership Council. This charter will expire in 2014, at the end of the month in which this Charter was approved.

(9) IPR POLICY: *The Organization approved Intellectual Property Rights Policy under which the WG will operate.*

Kantara Initiative IPR Policy - Creative Commons Attribution-Share Alike Option

(10) RELATED WORK AND LIAISONS: *Related work being done in other WGs or other organizations and any proposed liaison with those other WGs or organizations._*

Previous work related to the efforts of the WG includes: *(a) "Authentication 2.0: New Opportunities for Online Identification"*, by Center for Strategic and International Studies; (b) "*Online Identity Theft: Changing the Game"*, Microsoft Whitepaper; (c) "*Connecting Americans to their Healthcare: Consumer Authentication for Networked Personal Health Information"*, by the Connecting For Health Initiative of the Markle Foundation; (d) "*The ID Divide: Addressing the Challenges of Identification and Authentication in American Society"*, by the Center for American Progress; (e) "*Securing*

Cyberspace for the 44th Presidency", by the Center for Strategic and International Studies; (f) "*Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*", National Security and Homeland Security Councils

The WG may have liaisons with other WGs, including the Identity Assurance & Accreditation WG, Health Identity & Assurance WG, Privacy, Public Policy WG, eGovernment WG, and User Driven and Volunteered Personal Information Policy WG.

Other organizations that the WG may interact with include the Information Card Foundation, ANSI Identity Theft Standards Panel (IDSP), Center for Strategic and International Studies, Center for American Progress, Internet Society, Center for Applied Identity Management Research.

(11) CONTRIBUTIONS (optional): *A list of contributions that the proposers anticipate will be made to the WG.*

(12) PROPOSERS: *Names, email addresses, and any constituent affiliations of at least the minimum set of proposers required to support forming the WG.*

- Bob Pinheiro, Robert Pinheiro Consulting
- Pak Mark, Independent Business Investor
- Ron Carpinella, Equifax
- Alex Popowycz, Fidelity Investments
- Drummond Reed, Information Card Foundation