Data Verification Platform in a Nutshell

1. There is no such thing as identity theft.

After a data breach, a person's identity remains the same. What has been stolen, or rather copied, is a set of identifiers and other data about them.

2. Identity crime is actually about the copying and replay of data.

Criminals can re-use stolen data to impersonate people because the counterparties cannot reliably tell whether the identifying data is being presented to them by the real data subject or an imposter.

3. This problem can't be solved with more "identity" but only with better data.

Parties online need reassurance not only that the identifying data presented to them is correct and authentic, but that it is presented by the correct person, or under the control of the correct agent.

4. Digital wallets are powerful data containers, but they're incomplete.

Today's digital wallets can hold and release the cryptographically secured credentials needed for a given transaction. If we can make cryptographically signed credentials the way to present identifying data, then stolen identifiers are useless to criminals.

5. A wallet without a scheme is just a container of data that has no story.

The wallet must connect to a system of rules managing the entire data story to provide verifiable credentials. Apple Wallet, for example, has rules for every direct participant. Apple vets and onboards credential issuers with care and under contractual obligations.

6. We propose a network business model to share verifiable data.

The DVP business model introduces a new kind of player, a *data distributor*, which brings together the sources of the data, which we call the *data origins*, with the risk owners which rely on the quality of that data, enabling a two-sided market for data sharing. The entire scheme is overseen by the DVP operating organization, building consumer trust through globally recognized branding.

7. The risk owner is the ultimate consumer of verifiable data.

The needs of the risk owner drives the DVP model. Risk owners select the credentials they need, the DVP gathers subject's permission, and the data distributor gathers and returns the credentials under standard contractual agreements.

The DVP is the key to getting meaningful verifiable credentials, real facts, into and out of wallets and making those facts accessible to a potentially global market of risk owners.

version 0.7-US, March 22, 2023