THE MESS THAT NEEDS FIXING

A brief tour of four examples, in one video.
(Three of these examples have longer videos to back them up)

We speak of *measurably reliable identities*, and the Attestation Officer's central role in creating them. Most of today's problems with the Internet are rooted in the LACK of *measurably reliable identities*. [dog cartoon] Which means [big equal sign] -- a pervasive lack of ACCOUNTABILITY. [Scene of threats/blank heads/ overlaid with a big WHO DID IT?] with fraud, theft, breaches, and other attacks launched daily by perpetrators with little worry of exposure.

Here are some examples:

SPEAR-PHISHING

A huge proportion of today's cyber-attacks start with an email that makes a phishing or spear-phishing incursion by bad actors who are getting better and better at infiltrating a company's network and engineering an insidious surprise attack from within. [Ripped headlines.] By designing email systems that separate digitally signed messages from unsigned – and therefore untrusted – messages, phishing attempts are flagged right at the gate.

Measurably reliable identities enable the digital signatures that will solve the email phishing problem.

POROUS CORPORATE NETWORKS

[From the white paper "Have Identities Before You Manage Them"]
Organizations haven't kept up with the expanding pool of people who may have access to their networks. Who ARE all those people in your network?
Contractors? Suppliers? Distributors? Customers?
A widely dispersed collection of people with whom you never rub shoulders are in there, looking at files and installing software.
inauthenticity anywhere in the network makes the entire network less trustworthy and therefore less useful.
You need to know with a reliable measure of certainty just who those people are.

Measurably reliable identities provide the foundation for secure access management, to make sure only known, accountable individuals are allowed in.

SYNTHETIC IDENTITIES

Biometrics! The gold standard for personal identification, right? Well, yes and no. Biometrics ARE very reliable. ~~we don't need better biometric technology.~~
Biometric data represents a real human being, that's true.
But wait – How is that biometric data actually *linked* to that human being?
As it turns out, biometric data is often stored on a *smart phone* that is OWNED by that human being.

Now suppose that person buys more phones and sets up his biometrics on every one of them, creating multiple versions of himself. He can now set up a phony name and financial profile for each one, get a credit card for each one, and go on a spending spree. Each one looks like a legitimate customer to his bank – after all, he signs in with his real face scan or fingerprint on whichever phone identity he is using to buy the next car or diamond ring.

This scam of multiple identities -- called "synthetic identities" – is spreading in the worldwide banking industry, enabled by the pervasive – and WRONG – assumption that biometric identification is foolproof. ~~You don't hear about it because banks are loathe to admit they have no way to prevent it and would rather write off the fraudulent debt than expose the vulnerability.~~

Measurably reliable identities, attested to by an attestation officer, will thwart this scam by assigning an identity quality score (IDQA) to every identity certificate, and banks will require an Osmio VDR credential with an IDQA score of a certain minimum value to ensure the identity is valid.

Synthetic identities cannot exist in an environment of measurably reliable identities.

FAKE NEWS

[Including fake videos]

The line between reality and fiction is fading fast, with the proliferation of media platforms with ever more sophisticated attitude tracking, targeted messaging, and like/share viral epidemics. Not to mention technology that can now create videos that obliterate the reality/fiction boundary. Digital signatures of *measurably reliable identities* will not only ensure the identity of an author – providing *accountability* for the source of a news item – but will also flag altered content.

In these examples – as with almost all kinds of breach, fraud, theft, and crime – it's measurably reliable identities of *real people*, backed by a community of Attestation Officers (also *real people)* that provides the solution that **works**. Authenticity in the digital age – call it *The Internet of People* -- is based on time-tested paradigms from earlier times, brought forward with the help of technology such as PKI, IDQA, and IoPP [one-line explanation of each of those].