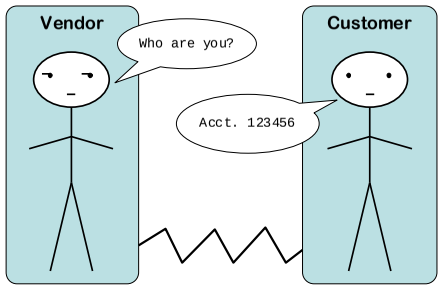
How to stop ID theft

Safety in numbers

The root cause of most identity theft (or more correctly, *identifier* theft) is the carefree way in which online businesses ask for – and get – our personal numbers. The ease with which numerical identifiers can be taken over and replayed has created a crisis of confidence in authentication, and regrettably, an ever worsening tide of private data being exchanged and exposed.

The identity crisis

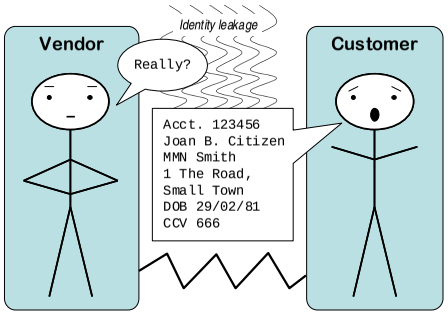
Look at the typical call centre transaction. The operator starts by asking your account number.



But it's not enough to identify you, so they need corroborating details, such as your full name, date of birth and password. And your spouse's name, your mother's maiden name, your mailing address and your credit limit.

Presenting this rich identity portfolio is made necessary by the fact that your account number cannot be trusted when quoted in any online channel, be it a call centre or website.

The worse ID theft gets, the more identity data is demanded, and the crisis only deepens.



The current situation endangers all players:

- it creates rich veins of personal information that fuel ID theft and cyber-crime
- it damages the privacy of consumers
- it does nothing to stop counterfeit identities.

What really matters about online ID?

The receiver of an online ID or customer reference number really only needs to know two things:

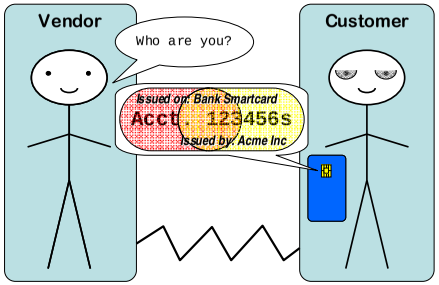
1. the number presented is genuine, and
2. it has been presented afresh with the owner's consent, not stolen and replayed.

Lockstep Technologies' *Stepwise*

Stepwise uses built-in public key security features of personal authentication devices to encapsulate customer reference numbers, identifiers and so on. *Stepwise* enables each personal number in turn to be cryptographically sealed with two vital pieces of information:

1. the issuer of the number, and
2. the fact that the number was carried in a particular *type* of device – such as a smart credit card or a SIM card – without revealing which device.

Each ***Stepwise*** capsule is effectively a de-identified notarisation of the user and a reference number. The relevant notarisation can be presented and bound by digital signature to such transactions as payment instructions, credit card orders, e-health records, and Internet voting. ***Stepwise*** works with a variety of devices including smartcards, mobile phones and USB keys.



Stepwise is compatible with a range of existing smart-cards, including FIPS 201 and DDA-capable EMV chips. The technical requirements are on-chip PKI digital signatures and key generation, and a CMS that permits post-issuance digital certificate loading.

Benefits of *Stepwise*

- **identifiers cannot be stolen and replayed; a copied ID is worthless without the user's device**
- **no extraneous details are needed to establish the user's bona fides; transactions can be trusted by virtue of a customer reference number alone**
- **transactions can be entirely de-identified**
- **multiple numbers can be independently sealed in the one device, with no central linkages**
- **solution can be deployed to most PKI enabled cards via the CMS, requires no card applets.**