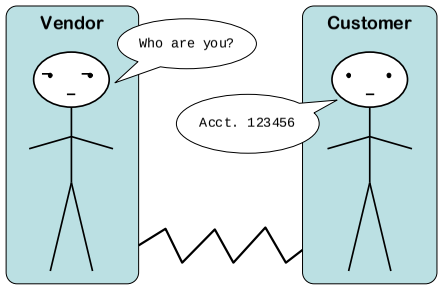
# We can stop ID theft!

## 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.

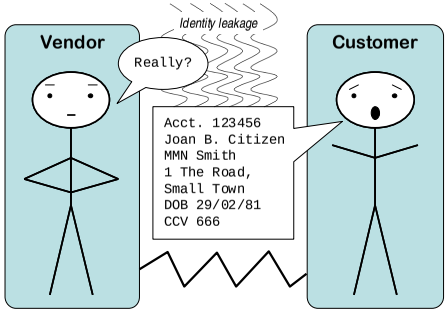
## The identity crisis

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. For instance, e-commerce sites increasingly want the CCV number from the back of your credit card. The Credit Card Verification number was introduced to combat "dumpster diving", the dominant modus operandi of identity thieves pre-Internet. But with CCV numbers now being quoted so freely, their security benefit has all but evaporated.

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?

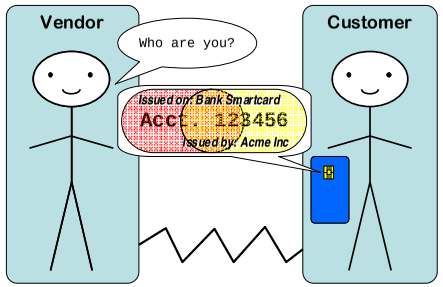
The receiver of an online ID really only needs to know two things:

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

## Lockstep Technologies' *Stepwise*

***Stepwise*** uses native public key security features of modern smartcards and similar devices to encapsulate identifiers. Stepwise enables each unique ID and each transaction to be sealed with two vital pieces of information:

1. the issuer of the ID (which need not be the issuer of the device), and
2. the fact that the ID was carried in a particular *type* of device (without saying which device).




***Stepwise*** can de-identify and secure such transactions as Internet banking, e-health and e-voting. ***Stepwise*** works with a variety of devices including smartcards, WPKI phones and USB keys.

## 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 the relevant identifier alone**
- **transactions can be entirely de-identified**
- **multiple IDs can be independently sealed in the one device, with no central linkages.**