Technology Scapegoats and Policy Saviors

Fred B. Schneider
Associate Editor in Chief

Just because technology creates a problem doesn't mean that it can provide a solution. And just because technology is involved, doesn't mean that it's the cause. These lessons are largely ignored in today's discussions about how to reduce the frequency and costs of identity fraud and identity theft. As a result, we're getting nowhere. Today's technology can solve this problem; a lack of incentives for deploying that technology is the difficulty.

In *identity fraud*, a criminal obtains information about a victim and uses this information to impersonate and charge purchases to the victim's accounts; with *identity theft*, the criminal creates new accounts or other business relationships (unbeknownst to the victim) and uses them for purchases or other actions attributed to the victim. Either can defraud a seller (or an intermediary, such as a bank or credit-card provider) who provides goods or services but is paid neither by the criminal (whose identity is unknown to the seller) nor the victim (who rightfully disavows the purchases). And either can defraud the victim who unwittingly pays a bill for a specious charge but later is unable to get a refund because goods or services were delivered as requested. Both crimes have reached serious proportions in the US and the UK, and they seem to be a growing concern elsewhere in the world (although observed differences across countries and cultures remain unexplained).

Defrauded sellers typically roll their losses into their cost of doing business, in effect recovering costs of identity theft from honest customers. Victims incur a loss of reputation and tarnished credit ratings, which are restored only by investing a great deal of time and effort in setting the record straight, both with defrauded sellers (many perhaps unknown to the victim) by canceling orders for goods and services the victim never purchased, and with credit bureaus and other institutions that have erroneously attributed fiscally irresponsible actions to the victim. Time is money, so dealing with identity fraud and identity theft can be quite expensive for its victims.

One way to eliminate identify fraud and identify theft would be to somehow prevent the identifiers commonly used to open financial accounts from being misappropriated. With this goal in mind, we as consumers are admonished to protect ourselves by keeping secret our social security numbers, credit-card numbers, bank account numbers, and mothers' maiden names. Legislation enacted in California (with variations subsequently passed elsewhere) incentivizes businesses to better protect files that contain such identifiers, so data breaches are less likely to give criminals access to this information. A recent US Government Accountability Office report, however, notes the absence of evidence to connect data breaches with identity theft.[1] Numerous data sources help criminals commit identity theft, and we have little understanding of where they're getting the credentials they use.

Arguably, a second approach to solving the problem would be to find and prosecute the various perpetrators of identity theft and identify fraud. This, unfortunately, isn't currently feasible because our networked systems don't enforce the strong authentication necessary to establish accountability of actions. What about shutting down the Web sites and chat rooms in which identity data can be purchased? Although this certainly could improve things, it requires ongoing vigilance and never eradicates the crime; as such, it's a losing game.

However, we can win by limiting the utility of "stolen" identity information. If the personal information that thieves can procure from electronic databases, unsolicited offers of credit grabbed from mailboxes, or old-fashion dumpster diving were insufficient to steal someone's identity, then "theft" of that information would be less problematic. Today's practice of authenticating a person by asking for an identifier (something that, by definition, can't be a secret) is fundamentally flawed; institutions that use this practice are being irresponsible. Social security numbers and other routinely available personal information shouldn't suffice to authenticate an individual, but today it often does. Sellers and other institutions need to change that.

The improved regime, however, would doubtless be more costly.

New programming and possibly new hardware would be required if stronger methods of authentication were adopted, because user authentication would now involve a secret, a token, and/or a biometric measurement; in addition, users would find the task of authenticating themselves prior to performing a transaction more onerous.

Given that they pass their costs to consumers, institutions have little to lose if they all adopted stronger means of authentication. (Were only some to make the switch, however, identity theft would likely continue—some users would opt to trade convenience for security by choosing institutions that implement weak authentication.) But institutions also have little to gain by adopting stronger authentication because they currently don't suffer the losses for identity crimes. Not surprisingly, they haven't switched to stronger authentication.

Independent of how various institutions would fare in isolation, society would certainly be better off with reduced levels of identity theft and identity fraud. Governments usually step in when we, as individuals, lack the power to compel behaviors required for the greater good of our society. And we as individuals do lack the power to incentivize the needed investments in better authentication.

Matters of procedure and policy—not the need for new security discoveries—is what allows identity theft and identity fraud to continue. The absence of greater institutional investments in better authentication systems and practices, in effect, makes our institutions accessories to the crime. It's time to acknowledge this culpability and foster its elimination through regulation, legislation, or other forms of public policy. Policy makers must create a climate to facilitate the deployment of stronger authentication and associated practices. □

Reference

1. US Gov't. Accountability Office, *Personal Information: Data Breaches Are Frequent but Evidence of Resulting Identity Theft Is Limited; However, The Full Extent Is Unknown*, GAO-07-737, June 2007; www.gao.gov/new.items/d07737.pdf.