Cost of Identity Theft

By Marc Samson
February 7th 2004
CEO Intelligent Switched Systems

Identity theft is a growing issue, for individuals, companies and government. Last year 10 million people were victims of identity theft. Victims spent on average 175 hours to clear their names and incurred a cost of over $1100 (USD). The Federal Trade Commission in the United States estimates that it takes victims 14 to 16 months to clear their names.

There are a large number of services that are built on simple access of account number and PIN. To be fair, many of these date back to a time when current criminal activities were not envisioned. But the fact is we do have many new forms of crime, and these need to be met with new solutions.

No one wants to do less business, on the contrary every one wants to do more, with lower costs to achieve the business, but at what cost? More and more companies are dealing with customers they simply have no face to face contact with. The transaction is either over the phone, or over the internet. The issue then who is "the customer". This comes right to the heart of identity theft. More and more companies simply do not know if the person is who they say they are. Some companies have policies and procedures in place in an effort to deal with this situation. One method is to only ship product inside the country where they operate, but this is fine for criminals, they are will to oblige with simple constraints like that. The major credit card issuers have added 3 extra digits on the back of the card in an effort to prevent fraudulent use of the card, but it is still a fixed number, and once it is compromised it can be used.

Smart cards are a very effective tool in combating identity theft. They offer very strong security, and are very easy to use in smart card reader equipped devices. One of the major issues with them, is not all devices are smart card reader equipped, nor is this envisioned any time soon.

There is a device which does have a very high degree of penetration around the world, and can be used as an access device. That is the telephone (regular phone, or cell phone – mobile phone). An audio token can be used to send a one time password over the phone. This is done by holding the token up to the phone, and activating the token to send a one time password. The next time the token is activated a new password will be sent. The obvious point is if some one steals the token, then they have stolen a person's identity. It is for this reason that the authentication must be a combination of the one time password from the token, and a PIN or password that the user enters on the keypad. Or in simple terms, what you have and what you know.

The last thing that people want is another device to carry around. The most convenient format for the token is to have it in the current card for the service it will be used with

(credit card, Medicare card, employee ID card,…) This has the added advantage that it is a card that will be used with all the other interaction in that service space, and hence the user will notice if the card has been stolen.

This is not technology of science fiction, but rather a reality of today. This type of security was installed by the ICAO (International Civil Aviation Organization) in a response for increased security following the events of 11 September 2001 in the United States of America.

The cost of identity theft hurts every one. It directly affects the individual who have had their identity compromised. It also directly affects all the companies and institutions that person has a relationship with as they have to dedicate their time and resources to assist the individual to recover and repair their identity. And it affects the public at large, as in the end they bear the cost that companies and institutions incur as a result of identity theft.

marc@iswitched.com