Dilemmas of Online Identity Theft

Omer Mahmood
Charles Darwin University, Australia

INTRODUCTION

Identity theft is a rapidly growing problem in the electronic environment. It has been recognized as the most widespread and fastest growing crime in the United States (Ahern, 2003). It is of great concern to online users, online service providers, governments, and law enforcement agencies. Identity theft could happen as a result of highly specialized electronic attacks (Sweeney, 2005), bugs in the system of the service providers, physical theft, misplaced paperwork, or just because of human negligence. Victims of identity theft sometimes spend considerable time and money to fix the problem; however their personal loans, mortgage, credit cards, and car loans can still be refused (FTC, 2002). This is shattering the confidence of users, thus creating a distrustful environment while making it very hard for small and medium-sized online service providers to compete with both established online and physically present service providers.

Various governments and law enforcement agencies are introducing tougher data protection and data security breach notification acts. These are increasing the operational costs of small to medium-sized online businesses, so it is becoming hard for them to compete with eBay merchants, and online and international specialized sellers. Even though small and specialized merchants provide better economic benefits to users, they are restricted from materializing business goals due to lack of trust in their infrastructure and absence of privacy policies. In this article a conceptual model is proposed as the future direction to protect the end user from possible online identity theft. The proposed conceptual model is based on the notion of having a trusted third party in between the user and the seller.

IDENTITY THEFT

The Identity Theft and Assumption Act was passed by the U.S. Congress in 1998, making identity theft a federal crime in which one:

> *Knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law.* (U.S. Congress, 1998, p. 1)

The above definition by U.S. Congress clearly states that identity theft is directly related to unlawful use and exchange of personal information to commit any illegal activity.

Categories of Identity Theft

Foley and Foley (2005) defined three main categories of identity theft:

- **Financial Identity Theft:** The perpetrator uses the victim's identifying personal information to open accounts such as bank accounts, credit cards, car loans, or even to rent a property.
- **Criminal Identity Theft:** The victim's information is provided to the law enforcement agencies by the criminal instead of his or her own when required.
- **Cloning Identity Theft:** The victim's information is used by the perpetrator to set up a new life. In this case the perpetrator usually uses the victim's information to steal his/her professional establishment or for illegal migration.

Economic Impact

The diverse methods used to steal the identity of a person in an online environment are continuously changing and include use of computer viruses, "worms," keyloggers, and spyware software. Recently, *phishing* and *pharming* attacks have also emerged. Another type of theft includes theft or loss of a company's unencrypted backup tapes, laptops, and documents. For example, on June 2, 2006, Hotels.com warned that due to the stolen laptop of an Ernst & Young employee, some 243,000

customers' names and credit card details (Bouldton, 2006) could have been stolen. Such growing diverse attacking techniques, incidents, and their frequency create new challenges for corporations all around the world who need to invest huge amounts of resources to protect customer information. These information protection techniques require large sums of investment, which most of the small and new merchants cannot afford, thus creating a sense of insecurity among customers. Identity theft-related costs are also prompting governments to introduce new, tougher laws—such as the Database Breach Notification Security Act ("SB1386") of California—which are putting more responsibilities on the shoulders of the corporations while increasing their workload and operational costs. This act enables government agencies to impose a fine of $50,000 or less per day to a company that collects personal information but fails to notify the clients of a data security breach or unauthorized access to their information (Internet News.com, 2005). In order to reestablish users' trust in the electronic environment, a solution is required. Such a solution would enable the users to have full control of their personal information, to apply restrictions on their data, and to store their information in encrypted format at one location rather than it being replicated and distributed to various companies and organizations.

Emerging Business Models

Unified platforms like Amazon and eBay are changing the way we learned to buy goods and services online. Both companies provide access to monetary insurance to their customers and have dispute-resolution policies. Moreover, both companies facilitate the end user to search for a product or service and provide feedback on the sellers, a standard user interface, and optional access to enhanced monetary insurance services like PayPal. Such unified online platforms like eBay and Amazon are making it tougher for the large online merchants to compete with the small specialized merchants who do business under the umbrella of established brands like eBay and Amazon.

However even the e-merchants who operate under the umbrella of established brands like eBay and Amazon have failed to utilize and materialize their business potential, as they usually do not have a privacy or disclosure policy. Moreover they generally do not have the appropriate infrastructure and specialties to ensure the confidentiality of the data collected from the users. Such vulnerabilities increase the user's perceived privacy and data security risks, and restrict the users to commit online transactions.

Although PayPal assures that it does not share the user's credit card and account details with other parties to ensure the confidentiality of the user's bank and credit card details, the data regarding the e-mail and postal address of the users is shared and stored locally by the small merchants for order processing and record keeping. However, it has been reported repeatedly that information is stolen/lost by the big corporations like PayPal and Time Warner due to inadequate security measures and procedures (Mutton, 2006; Silver, 2005).

Therefore a solution is required that will enable:

1. online users to take full control of their information
2. online users to see the logs of their information access
3. online users to keep their personal data at one secure central repository, so that it is easy for them to maintain and update and
4. online merchants to save in terms of operational costs, as they will not be required to set up and maintain secure database servers in order to store customers' personal information

On the other hand the solution should enable the merchants and service providers to access the information from a secure repository:

1. after getting the user's explicit permission
2. for the permitted time period and
3. for a user-specified number of times

Such a solution will enhance the user's level of trust and confidence in committing online transactions, as they will know that their private information is not stored at various locations and they are not likely to suffer due to the negligence of others.

PROPOSED MODEL ARCHITECTURE

Technical models have been proposed to tackle the problem of identity theft by combating certain types of data theft techniques such as phishing and pharming