

P E R S P E C T I V E

## ID Theft – Proliferation and Safeguards



YOUR INNOVATION PARTNER

## The Many Avatars of ID Theft

Consumers of the digital age have to safeguard one more item besides cash, credit cards and valuables – their identity! ID theft is the fastest growing crime in the United States, where one such incident occurs every four seconds. A leading financial services research firm claims that ID fraud touched nearly US\$ 50 billion in 2009 and affected over 10 million Americans. A senior executive from the firm maintains that the numbers will remain high until unemployment and economic pressures ease.

Broadly, ID fraud refers to the theft and subsequent misuse of a person's identity by another to commit money-related unlawful or outright criminal acts. This could range from a simple theft of an ATM card to making false loan applications, to money laundering and even terror financing.

The security of traditional modes of payment and verification have been compromised by tricksters using hardware and software to counterfeit cheques, skim cards, duplicate magnetic strips, hack user names and passwords etc. Now, the proliferation of online commerce and social networking offers miscreants ample opportunity to impersonate someone by stealing their personal information including name, Social Security Number, debit / credit card details and so on. Thus, Internet sites are becoming the favoured modus operandi of ID thieves, upstaging 'traditional' methods, such as stealing a wallet, 'skimming' a credit card or looking over someone's shoulder as he or she enters her Personal Identification Number at an ATM.

Phishing has also evolved beyond impersonation over email to a new technique called 'pharming', wherein the victim is directed to a 'spoof' website closely resembling the original and asked to divulge personal information. These sites usually return error messages, after storing the information for later misuse. And, 'crackers' are the newest breed of ID thieves who specialize in accessing computer hard drives remotely, over the Internet.

ID fraud is doubly dangerous than regular theft because it need not be a one-time event, and in the worst case, might persist for years. A thief may sell the stolen ID to another trickster or direct bills for fraudulent purchases to a different address,

making it all the more difficult to trace the crime. Many hapless victims have found to their dismay that timely reporting of the loss of their identification documents does not necessarily prevent them from being misused.

## The Hunting Ground of Tricksters

Most 'non-traditional' ID fraud occurs in the following three domains:

### E payment

Both financial institutions, seeking higher operating efficiency and consumers, seeking convenience, have driven the growth of online and mobile payments. Electronic payment modes have diversified to include account to account fund transfers, credit card-based Internet payments, Peer to Peer (P2P) payments, to name a few. Credit cards have always been a major target of fraudsters, who steal card-related information to rack up online purchases. In 2008, the sixth-largest payments processor in the U.S. was the victim of a sophisticated attack by hackers, who used sniffer malware to pick up names and credit card numbers from unencrypted transaction information transmitted over the company's internal processing platform.

Now, emerging payment modes including pre-paid cards and 'virtual world' transactions are attracting the attention of miscreants. Users of online P2P lending services are quite vulnerable to attack, since the providers are not yet adequately regulated, and therefore may not have instituted sufficiently stringent authentication measures to ascertain the identity of users of their websites. Criminals have been known to exploit these loopholes to impersonate genuine users.

E payments and online ID fraud work in a vicious cycle, each one feeding off the other. The popularity of online modes of payment adds fuel to the fraud fire; in turn, the lure of easy opportunity induces more and more tricksters to transact using electronic payments.

### Mobile payment

The mobile phone has done a lot more than facilitate easy communication. Mobile payments are replacing cash as well as credit cards. Another

new technology slated for launch later this year will allow anyone with an iPhone to accept debit or credit card payments immediately. While the convenience of mobile payments - made from a stored value account attached to one pre-paid mobile number to another - has made remittances accessible even to the unbanked, it has also provided fraudsters with one more avenue to ply their trade.

With no rules governing these transactions, criminals can assume fake identities and emails to acquire a mobile account from which they can transfer huge amounts of money for all types of illegal purposes from money laundering to terror financing. By disposing of the prepaid card after use, they can easily escape detection.

### Social media

Open platforms have led to the proliferation of mobile-downloadable applications, not all of which are bona fide. Rogue applications can escalate the threat of ID theft – recently, several Credit Unions were under a mobile phishing attack wherein tricksters wrote downloadable applications – branded with the Credit Unions' logos – to induce members to part with their financial information.

Profiles on social networking sites provide a lot of personal details which could be misused to create dummy accounts. Facebook has launched a P2P payment service in collaboration with UK's 'ClickAndBuy' that allows friends on Facebook to send and receive money. In the absence of sound KYC norms, it is not possible to verify that the money has gone to the person it was intended for and not to someone else masquerading as him or her.

Although such payment services have not yet assumed significant proportions, it is anticipated that social sites will be increasingly used as payment engines or platforms for online gamers to trade credits in the near future. Therefore, there is a strong need to bring these services within the scope of tight regulation.

### Collective Responsibility to Safeguard

The incidence of new account fraud underscores the need for banks to be watchful right from the origination stage. Numerous accounts opened by

the same individual or corporate customer, multiple related accounts in the name of a single financial services representative or trial deposits from other financial institutions could all be cause for concern.

On the channel innovation front, along with improving customers' access to their services and reducing Total Cost of Ownership, banks must redouble their efforts to ensure the safety of transactions conducted via mobile and the Internet. Strict user authentication measures, applied consistently across all channels including emerging modes, will go far in preventing unauthorized access to private data. Banks could rely on strong authentication based on a combination of 'What you know' like password or pin, 'What you have' like a smart card and 'What you are' like Biometric authentication. Mobile phones are already being widely used for authentication of online payments, including generating One Time Passwords (OTP) as second factor authentication. Though not popular today, third factor authentication based on biometrics, including finger print, voice recognition and iris scan are also being recommended. While techniques such as Multifactor, Out of Band and Biometric Authentication help filter out most identity theft malpractices, velocity-based fraud protection solutions monitor frequency and pattern of transactions to highlight suspicious activity. Financial institutions must also strengthen their monitoring systems. Through Adaptive Authentication, which is based on risk profiling, banks can safeguard their customers against ID fraud. Using this technique, banks can create a risk profile of their customers based on their normal usage pattern, transaction value, location and other behavior, and assess the 'risk score' for each. If a particular transaction appears riskier than usual, by originating in a high-risk country which is not the usual transaction location, for instance, a second level of online or telephonic authentication is applied to ascertain the genuineness of the same. Likewise, any transaction occurring at unusual times or suspicious IP addresses, or of a value higher than usual, is treated as suspicious, and customers are immediately notified of the same. In this context, fraud scoring analytics solutions, which identify patterns from historical data to create rules that help detect future fraud could prove useful.

Even within the organization, the flow of customer information must be strictly regulated through control mechanisms that permit access only to authorized personnel.

In spite of these safeguards, should ID theft occur, banks must act quickly to resolve the problem. They must accord top priority to freezing attacked accounts and responding to genuine requests for information from victims.

In general, ID verification systems must be tightly integrated with the other systems that participate in, or facilitate online transactions. By adhering to the regulatory policies in different regions, software systems can contribute to the mitigation of ID fraud. The use of best-in-class fraud detection and prevention tools can further improve the security of transactions. Identity Management Systems leverage stored information to authenticate internal and external users before authorizing them to proceed with a transaction. Banks that intend to deploy such a system to defend against ID fraud must select one that is not only secure but also user-friendly, allowing a person access to all authorized applications with a single sign-on.

The role of the regulatory framework is no less important. Taking cognizance of the situation, the U.S. Department of Justice has tightened legislative measures against identity theft and fraud, which are now liable for prosecution under multiple statutes, and attract hefty penalties or imprisonment up to 30 years. The machinery has been strengthened with Federal prosecutors working closely with other investigative agencies to initiate punitive action in cases of ID fraud. The higher incidence of ID fraud in serious crime may necessitate further tightening of Anti Money Laundering policies.

Meanwhile, the Payment Card Industry Security Standards Council has taken safeguards against card fraud by standardizing data security measures to be taken by all organizations processing card payments. The Federal Financial Institutions Examination Council issued new compliance guidelines a few years ago on authentication standards for Internet banking, which broadly require banks to identify high risk activities and determine for which of these, single-factor authentication is inadequate.

People must also share the responsibility of safeguarding their identity. Banks frequently send out warnings about spam email, phishing and other malpractices, which customers ignore at their peril. Instead, they must adopt prudent financial practices

such as checking bank and credit card statements regularly, sharing private information only to the extent it is required and that too with bona fide agencies, transacting on well-known websites, safeguarding their ID documents, passwords and sensitive information, registering with a 'Do Not Call' registry to block unscrupulous callers and so on. They would also do well to subscribe to identity protection services such as credit monitoring, fraud alert and database scanning. And should the worst happen, customers must quickly call the authorities such as the Federal Trade Commission or local FBI office in the U.S., or the relevant agencies in other countries.

### Summary

ID theft refers to the misuse of stolen identity for financial gain. With the proliferation of online commerce, the incidence of ID fraud is on the upswing. ID theft is no longer the preserve of petty thieves; it has assumed ominous proportions, facilitating serious crime from money laundering to terror financing.

The emergence of new, loosely regulated payment channels on social networking sites and prepaid mobile phones has made it easier for fraudsters to carry on their activities. Effective and consistent regulation is therefore the need of the hour. Financial institutions must also strengthen their authentication processes, and make use of technologies such as Biometric, Multifactor and Adaptive Authentication.

But, perhaps the greatest responsibility lies with the users. By resorting to judicious financial practices, they can safeguard their interests and identity to a large extent. After all, prevention is better than cure!

### References

- 1) <http://www.javelinstrategy.com/2009/02/09/latest-javelin-research-shows-identity-fraud-increased-22-percent-affecting-nearly-ten-million-americans-but-consumer-costs-fell-sharply-by-31-percent/>
- 2) Javelin Strategy Report - 2009 Identity Fraud Survey Report, Feb 2009  
[<http://www.javelinstrategy.com/>]
- 3) Gartner - Magic Quadrant for Web Fraud Detection, Feb 2009 (<http://www.gartner.com/>)

- 4) Identity Theft: What to Do Now, Barbara Bedway, Jan 13, 2010
- 5) Section on Identity Theft on website of United States Department of Justice
- 6) Heartland Payment Systems, Forcht Bank Discover Data Breaches, January 21, 2009 Linda McGlasson, Managing Editor, [http://www.bankinfosecurity.com/articles.php?art\\_id=1168](http://www.bankinfosecurity.com/articles.php?art_id=1168)
- 7) Twitter founder Jack Dorsey launches iPhone payment product, James Quinn, US Business Editor, 02 Dec 2009 <http://www.telegraph.co.uk/technology/twitter/6713229/Twitter-founder-Jack-Dorsey-launches-iPhone-payment-product.html>

**Author**

**Arunnima B S**

Lead Consultant - Finacle  
Infosys Technologies Limited



YOUR INNOVATION PARTNER

PERSPECTIVE

Universal Banking Solution | System Integration | Consulting | Business Process Outsourcing

#### Infosys Technologies Limited

Plot No. 44, Electronics City, Hosur Road, Bangalore - 560100. India  
Tel.: + 91 80 28520261, Fax: + 91 80 28521747, e-mail: [finacleweb@infosys.com](mailto:finacleweb@infosys.com)  
[www.infosys.com/finacle](http://www.infosys.com/finacle)

Join us on Twitter, LinkedIn and Finacle Whiteboard at [www.infosys.com/finacle/networking.asp](http://www.infosys.com/finacle/networking.asp)

"COPYRIGHT NOTICE: Copyright ©2009 Infosys Technologies Limited, Bangalore, India. ALL RIGHTS RESERVED."  
Finacle logo is a registered trademark of Infosys and Infosys acknowledges the proprietary rights of the trademarks and product names of other companies mentioned in this document. Infosys believes the information in this publication is accurate as of its publication date; such information is subject to change without notice.