


By Frank W. Abagnale

The Complex Universe of Identity Theft



Effective, thorough protection is more than just “locking” up your data...

Identity Theft is a broadly-used term that has achieved consumer awareness, but the term itself does very little to impart the vast ways individuals are at risk on a daily basis. To have the most thorough and effective protection against Identity Theft, consumers should employ a combination of services to address each of their areas of risk. Affinion has assembled all of these components with its world-class suite of Identity Theft protection services.

YOUR PERSONAL INFORMATION – the very key to your identity – is likely to be compromised in the coming year. Estimates calculated in 2007 suggest that approximately 264 million pieces of other people’s personal information were exposed by identity theft or fraud¹ – that’s almost as high a number as the 2007 U.S. population of 301,139,947.² You may not necessarily become a victim of identity theft, but with your personal information readily available for anyone to use, the likelihood of becoming a victim increases exponentially. But, that’s the bad news.

The *good* news is our government has taken a reasonably proactive stance on

See “Universe,” Page 2



The Complex Universe of Identity Theft

Effective, thorough protection is more than just locking up your data.

From "Universe," Page 1

identity theft and fraud. In 2003, Congress passed the *Fair and Accurate Credit Transactions Act*, which amended the *Fair Credit Reporting Act* to provide potential victims of identity theft with certain rights and protections. At the state level, additional laws have been enacted to prevent identity theft. The key components of such legislation include the following:

- Consumers are allowed one free credit report from each of the three main credit bureaus (Equifax, TransUnion, and Experian) each year. (*Fair Credit Reporting Act*, § 612; 15 U.S.C. 1681j)
- Consumers who have a good-faith suspicion they have been – or are about to become – the victim of identity theft, can place a “fraud alert” on their credit file. A fraud alert stays on the consumer’s credit file for at least 90 days, and requires any potential creditor to contact the consumer at the phone number provided or take other reasonable steps to verify the identity of the person applying for credit. (*Fair Credit Reporting Act*, § 605A; 15 U.S.C. § 1681c-1)

• Consumers must now be notified by the responsible party (that possesses personal data) in the event their personal data has been, or is suspected to have been, exposed in a data breach (currently a law in 39 states).

A Fraud Alert is Not Enough

Fraud Alerts are a free service for consumers. When a Fraud Alert is placed on your credit file, credit grantors are required to take additional steps to verify that the credit application is not fraudulent. The Fraud Alert includes the consumer’s phone number, and creditors generally call the consumer, as this is the fastest and most secure method to verify that the consumer is the one requesting credit, not an impostor. Sometimes, creditors use alternative methods,

including challenging questions or requesting additional identification, to verify the application.

Fraud Alerts are getting a lot of press these days, perhaps driven by Lifelock Incorporated’s advertising campaign. Viewers watch in awe as Lifelock’s CEO doles out his Social Security number to the general public, confident in its security. Unfortunately, this creates a false sense of security as fraud alerts prevent only one of the three major identity theft attacks commonly waged against consumers.

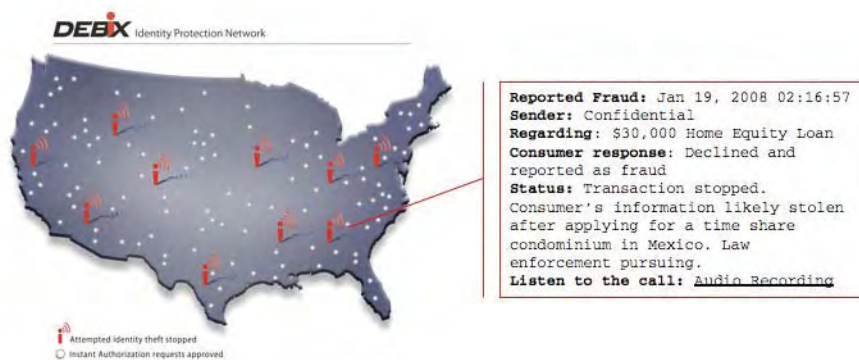
Lifelock’s business – like others providing undifferentiated services – is focused on setting Fraud Alerts. These limited service providers take this free, government-provided service and charge the consumer for it.

Affinion Group agrees that Fraud Alerts are effective and can be an important part of a complete identity theft solution. However, simply setting a Fraud Alert is not enough.

Debix – A Complementary Solution Inside Affinion

Affinion has entered into a partnership with Debix, the creator of the world’s

Figure 1: Debix in Action - Actual Crime Prevented



first and only electronic Identity Protection Network. This Identity Protection Network utilizes Fraud Alerts to allow banks to send an Instant Authorization to any consumer in the network.

Figure 1 illustrates the core capability of the Network. The white dots represent approved transactions where a creditor sent an instant authorization call, and the consumer approved it by verifying their VoiceKey after entering their 4-digit PIN into their pre-registered phone. In security jargon, this is called multi-band, multi-factor authentication. The red dots represent attacks where the consumer declined the account and reported it as fraud. The instant this report occurs, the consumer is transferred to a Debix call center to assess the situation and determine the proper course of action with law enforcement while the thief is still active. The network also provides an audit trail of the incident to support the case.

Never before have consumers, banks, and law enforcement been able to communicate in real time to prevent identity theft and pursue the criminals while the trail is hot. In the fourth quarter of 2007, Debix subscribers responded to 30,618 instant authorization calls from banks and also stopped 380 fraudulent accounts from being opened by reporting them as fraud. Of these, Debix escalated 29 hot cases to law enforcement as highlighted in Figure 2.

Limited service providers take the information from customers who want Fraud Alerts issued, and send the information to the credit bureaus. Their only follow-up activity is to re-send the information after 90 days, which is how long initial Fraud Alerts remain active.

Debix is the *only* company that is actually *with* the consumer during an actual account opening – fraudulent or not. The competition has no idea what is happening with the consumer’s identity.

Figure 2: ID Theft Attacks Stopped and Reported to Law Enforcement

	Instant Authorizations™ (automated requests from banks verifying a credit application is legitimate)	Identity Theft Stopped
October 2007	10,669	109
November 2007	10,256	129
December 2007	9,693	142



Affinion’s Complete Suite of Services

Affinion Group feels that Fraud Alerts can *help* combat identity theft, but they are *not* a complete solution because they address only one of the three common categories of attacks. For consumers wanting to take all possible steps to prevent identity theft, Fraud Alerts only help keep new fraudulent credit from being issued. They are useless when it comes to the other, more prevalent varieties of identity theft and fraud.

In November 2007, the Federal Trade Commission (FTC) published their annual report on identity theft. Through a survey of actual identity theft victims performed by Synovate Corporation, the FTC was able to determine three main categories of identity theft: **New Accounts & Other Fraud, Misuse of Existing Non-Credit Card Account or Account Number, and Misuse of Existing Credit Card or Credit Card Number.**

The Numbers Aren’t Pretty – and They Don’t Lie

Fraud Alerts do stop new fraudulent credit from being issued, which is the most damaging form of identity theft, but new account fraud is only estimated to be 22% of the identity theft problem. Non-credit account misuse and existing account misuse together represent nearly 78% of identity theft as reported by actual victims.³

Identity thieves will sometimes change the billing or mailing address on an existing account. They may also try to get new cards issued in their name or some other name. This is commonly referred to as “account takeover.” In

their report on identity theft, the FTC writes:

Account takeover was reported by 9% of victims who experienced existing credit card misuse, and 11% of victims who experienced existing non-credit card account misuse. Because new account fraud involves the creation of an entirely new account rather than the misuse of an existing one, account takeover does not apply to that type of identity theft.⁴

It is important to note here that limited Fraud Alert service providers do absolutely nothing to stop – or notify – a consumer that an existing account has been compromised. Currently, the only available means to detect account takeover is through regular monitoring of all your statements and credit monitoring.

Non-credit account fraud refers to fraudulent activities that do not involve the misuse of an existing or new financial account. In fact, 12% of victims reported non-account misuse – the most common form being a person’s name and/or personal information being given to the police when a thief was stopped or charged with a crime.³

Once again, limited fraud alert service providers like Lifelock will do nothing to protect or alert an individual of this type of identity theft. Detecting this type of fraud can only be accomplished through public information review and monitoring. There are hundreds, perhaps thousands, of identity thieves who won’t actually use your compromised

See “Universe,” Page 4

From "Universe," Page 3

personal information to steal your identity – they'll just sell it all to someone else who will. The sale of personal information generally takes place in underground Internet chat rooms. In fact, the President's Identity Theft Task Force and the U.S. Secret Service estimate there are 20,000 users of those underground chat rooms and "carding sites." Limited fraud alert service providers can't alert you if your personal information is exposed in these chat rooms. To date, the only reliable method of detection is real-time chat room monitoring.

Every Consumer Needs More Thorough Protection

There have been a number of governmental data breaches recently where state and federal governments have lost constituents' personal information. Despite the recent proactive federal legislation, these organizations have provided only part of the solution to help consumers protect themselves. While several government organizations have selected Debix to protect these consumers from new credit fraud, it is noteworthy that these organizations have not provided any form of monitoring for account takeover, public exposure of data, or non-financial account misuse. This is a particularly vital component when the compromised data includes constituents' credit card numbers, payment processing information, and other data that could be manipulated for account takeover or misuse. Remember, the FTC estimates these types of fraud make up nearly 78% of identity theft.³

For consumers wanting to take all possible steps to prevent identity theft, fraud alerts alone are not enough.



To have the most thorough and effective protection available, consumers should employ a combination of daily credit monitoring, public information monitoring and reporting, real-time chat room monitoring, and the Debix solution. Affinion has assembled all of these components with its world-class suite of Identity Theft protection services.

¹Privacy Rights Clearinghouse estimates 218 million records were exposed in 2007. This number does not include the TJX customer breach in which information from at least 45.7 million credit and debit cards was stolen.

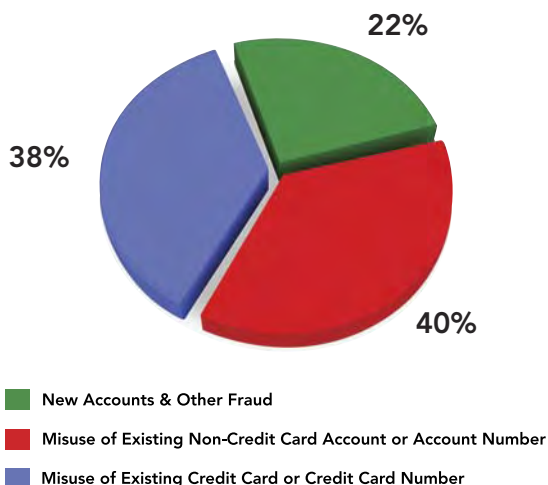
²<https://www.cia.gov/library/publications/the-world-factbook/print/us.html> (July 2007 est.)

³Consumer Fraud and Identity Theft Complaint Data, January – December 2006, Federal Trade Commission, February 2007

⁴Federal Trade Commission – 2006 Identity Theft Survey Report, November 2007

⁵Combating Identity Theft, a Strategic Plan. The President's Identity Theft Task Force, April 2007

Figure 3: Percentages of Identity Theft by Type



The three main forms of identity theft and their frequency, as determined by the Federal Trade Commission, through a survey of actual identity theft victims.