



## National ID Recovery, LLC

### “Nations Largest Identity Theft Case”

By: Adesola Badon

The US Department of Justice has just identified and indicted 11 people who they proclaim were the culprits of the nations largest identity theft scam in history. The eleven suspects, three of which were American, defrauded several retail companies out of at least 45 million credit and debit card numbers; they consequently accessed more than 1.5 billion dollars in funds that were available on these accounts. The men allegedly had been gaining access to these accounts since March of 2006 and had account information that dated as far back as December of 2002.

The suspects gained access to the retailer’s data through a technique called “war driving”. War driving is when a laptop is used while driving near the vicinity of a wireless network, then connecting to the network and installing a “sniffer” program to intercept and record transmitted information across the network. After obtaining the card information, the suspects then sold the information over the internet on credit card trafficking websites for profit. It was released that two of the suspects named, Maksym Yastremskiy of

Kharkov, Ukraine and Aleksandr Suvorov of Sillamae, Estonia, personally pocketed 11 million dollars in stolen funds from a well known New York restaurant.

The retail companies that were victimized by this breach included names such as DSW, TJX, BJ’s Wholesale Club, Office Max, Boston Market, Sports Authority, Barnes & Noble, and Forever 21. Three of these chains already have previous charges that brought action by the FTC due to their lack of safeguards to protect consumer information. It has not yet been reported by the FTC what action they will take in reprimanding the companies, if any, following the outcome of this case. Last years identity theft victim count soared to approximately 8 million victims and 2008 promises nearly 10 million. This case alone has potentially created more victims (known and unknown) than the last five years combined.



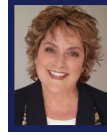
### In This Issue, You Will Learn About:

- > Nations Largest ID Theft Case
- > Consumer Reports: Wi-Fi Hot Spots
- > Recent Data Breaches

### Inside this issue:

<b>Nations Largest ID Theft case</b>	<b>1</b>
<b>Wi-Fi Hot spots</b>	<b>2</b>
<b>Data Breaches</b>	<b>3</b>

**Wi-Fi Hot Spots**  
**By: Consumer Fay**  
[www.consumerfay.com](http://www.consumerfay.com)



It's the end of a long work week so you stop in your favorite local java joint to indulge in your favorite pass time, rest and relaxation. Maybe you'll even finish up some reports from work or just surf on the internet. Coffee shop wireless internet in your mind, is the greatest invention known to man at this point; the smell of savory beans and the world wide web is at your finger tips. You flip open your laptop, fire it up, type in the code you have been provided for wireless access and viola....you're in business!

### <<SECURITY BREACH!!!>>

The alarms begin to sound off, all the doors in the shop lock to contain the perpetrator, and thank goodness all your important information is retrieved and returned to you safely and uncompromised; right? Wrong!, I'm afraid that could only happen in the movies. The reality is that your information is possibly in jeopardy in any "hot spot" location and honestly your privacy most likely has been compromised if you are a

frequent user of wireless hot spots.

Unfortunately most wireless hot spots are unsecure and easily accessible to any and everybody who wants to take a crack at intercepting your personal information. This problem occurs because in order to secure a wireless network a "private" encryption key or WEP key must be created for users. Since this key must be given to the public users in order to use the network to begin with, it inherently makes the encryption useless. Think of it this way, if you redo all the locks to your house to detour theft, but leave your new set of keys hanging from a hook on your front door, what difference does it make that you have new locks?

Wireless hackers use a multitude of programs and tools in order to capture your personal data. These include things such as sniffer programs, key logging software, or even going as far as to set up bogus networks to mimic the hot spot networks. A sniffer program is a software

application or computer hardware that can intercept and record traffic passing over a wireless network or part of a network. As goes across the network, the sniffer captures each packet and eventually decodes and analyzes its content. Key logging software is a method of capturing and recording user key strokes. This software is mainly used as a means to obtain passwords or encryption keys and thus bypassing other security measures. Bogus hot spots are usually access points that are set up near a wireless network to mimic and clone the look and feel of a nearby hot spot. In doing this it enables the administrators of the bogus network to steal account information and payment information from the legitimate network as well as steal any personal data that may come across the network.

You are always vulnerable when on a public network. Make sure to take the necessary steps to secure your private data.

Consumer Fay is a long time consumer advocate who provides info and ways to become even smarter buyers for all products and services. Fay's background is in the Consumer Electronics, Appliance, Photographic, Computer, Service Contract and other consumer goods Industries, along with consumer protection groups and associations over her 30+year career. She is a 4 time CEO who understands how business should be done. She has done 4 start ups – all successful and was a VP for RCA a while back, when they owned NBC.

Fay serves on several major Industry Boards, Committees, and Councils, and continues her long association with BEAR –Department of Consumer Affairs. She has the keen ability to develop long term and growth oriented businesses and partnering relationships while always keeping a sense of humor. Her business experience and organization affiliations allow her a unique perspective for providing consumers with invaluable information. Visit [www.consumerfay.com](http://www.consumerfay.com).

## Published Data Security Breaches Reported for 2008

There have been approximately 300 Published Data Breaches since January potentially exposing more than 12.5 million individuals to identity theft.

Date	Company	Type of Breach	Citizens Exposed
6/6/08	Stanford University	Stolen Laptop	72,000
7/2/08	University of Nebraska	Hacker	2,035
7/2/08	Baptist Health	Employee Theft	1,800
7/7/08	FL Agency for Health Care Administration	Security Breach	55,000
7/8/08	Yan Chai Hospital	Lost Backup	3,002
7/8/08	LPL Financial	Hacker	10,219
7/9/08	Wagner Resource Group	Peer To Peer File Sharing	2,000
7/10/08	Williamson County Schools	Accidental Online Exposure	17,000
7/11/08	Baxter International	Stolen Laptop	6,900
7/12/08	Indiana State University	Stolen Laptop	2,500
7/14/08	Missouri National Guard	Unknown	2,000
7/14/08	Washington Metro. Area Transit Authority	Accidental Online Exposure	4,700
7/17/08	University of Texas at Austin	Stolen Backup Tape	2,500
7/17/08	University of Maryland	Accidental Inline Exposure	23,000
7/23/08	Sealaska	Stolen Information	19,000
7/24/08	Hillsborough Community College	Stolen Laptop	2,000
7/24/08	St. Mary's Regional Medical Center	Data Base Breach	128,000
7/24/08	Village of Trinley Park	Lost Backup	20,400
7/26/08	Conn. College Wesleyan Univ. Trinity	Hacker	2,815
7/26/08	Indiana State University	Stolen Laptop	2,500
7/28/08	Macy's	Security Breach	4,100
7/28/08	Moraine Park Technical College	Systems Breach	4,400
7/29/08	Blue Cross, Blue Shield of Georgia	Hacker	202,000