



IFI Newsletter

A quarterly newsletter from Identity Fraud, Inc.

ISSUE #10 - October 2004

1. Largest ID Theft in the United States
2. Identity Theft Bills Reach Michigan
3. Five Charged in Theft of Navy Officers' Identities
4. Computer Worm Puts Cal Poly Students at Risk

Largest ID Theft in the United States

After Months of investigations, Kevin Barrows, a special agent for the FBI could not leave empty handed after he and a team of agents had spent several hours searching every room in the house, yet they had not found one piece of evidence.

So he headed back upstairs for a second look, and he focused his attention on an expensive canopy over the bed. When he pushed at the draping, he found that it was weighed down with files. They contained reams of financial information about hundreds of individuals whose identities had been stolen in a scheme that netted more than \$50 million dollars.

Two years later the home emerged as a linchpin in what law enforcement authorities describe as the biggest case of identity theft ever uncovered in the US. It was masterminded by just two people. At least 30,000 people nationwide were victimized.

Per Mr. Barrows, "The execution was seamless, and if they had been smart enough not to use a phone line that traced back to that house we probably never would have found them."

Free Credit Reports Available On The Following Dates

December 2004 – AL, AR, CA, CO, HI, ID, MT, NV, NM, OR, UT, WA, WY

March '05 – IL, IN, IA, KS, MI, MN, MO, NE, ND, OH, SD, WI

June '05 – AL, AK, FL, GA, KT, LA, MS, OK, SC, TN, TX

September '05 – CO, DE, DC, MA, MD, MA, NH, NJ, NY, NC, PA, RI, VT, VA, WV, Puerto Rico and US territories

Identity Theft Bills Reach Michigan

Legislation intended to strengthen protections against identity theft in the state of Michigan has been sent to the full Michigan House by that body's Criminal Justice Committee

The nine committee members voted unanimously to send a total of 18 measures — ten House bills and eight bills passed by the Senate — for consideration by House legislators.

The new legislation would make it a felony to steal and use another person's identity — or items, such as credit cards, that are personally identified with them — to purchase goods or apply for a job. The crime of identity theft would be punishable by up to five years in prison and a fine of up to \$25,000.

Five Charged in Theft of Navy Officers' Identities

Five men including a Navy petty officer based in Virginia have been charged with involvement in a fraud ring that used the stolen identities of Navy officers to buy thousands of dollars worth of merchandise from stores in the Baltimore area.

Between June and November of last year, authorities say, five Baltimore area men used the identities of some 20 Navy officers to fraudulently obtain credit accounts at such stores as Home Depot and Target.

Baltimore County police are currently investigating whether the Petty Officer was responsible for stealing the Navy officers' identities. In addition, he is accused of multiple violations of military law, including larceny of a car, larceny of a motorcycle, making a fraudulent purchase more than \$100, wrongfully using a government computer, and theft.

Computer Worm Puts Cal Poly Students at Risk

A worm that infected a computer at California Polytechnic University in San Luis Obispo has put some of Cal Poly students at risk of identity theft.

The intrusion was discovered when an abnormally high level of spam was noticed by an employee of the CSU Chancellor's Office and subsequently traced to a computer in the California State University (CSU) system. The Cal Poly computer was immediately taken offline and examined. That examination led University officials to the discovery that the computer had been infected.

University officials say the file — which included names, Social Security numbers, local and home addresses, and telephone numbers for 652 Cal Poly students — was placed on the computer by mistake.

The possible compromise of personal data is the second incident involving the private information of Cal Poly students and staff. On 28 June, an internal auditor at CSU noticed that his laptop computer's hard drive had disappeared from a locked office at the San Marcos campus. The missing hard drive contained names and Social Security numbers for about 13,000 Cal Poly students and employees, as well as information for students and employees at six other CSU campuses

IDENTITY FRAUD, INC.

Engaging Solutions for Identity Protection!

www.IdentityFraud.com

Email: info@identityfraud.com

© 2002 -2004. All Rights Reserved.