

## The Retail Store Hacker Albert Gonzalez Now Faces Prison Time

Topic: [Criminal Law](#)

From conviction of credit card fraud to participation with the Secret Service then back to being federally prosecuted again, Albert “Soupnazi” Gonzalez is facing a lawsuit in what could possibly be the single largest and most complicated identity theft crime in the United States.

In the past three years, Albert Gonzalez from Miami has managed to amass millions of dollars by breaching the U.S. retail networks, gaining access to credit and debit card numbers and then selling them.

### How Albert Gonzalez Fooled the Secret Service

**Gonzalez was offered a position to cooperate as an informant with the Secret Service in 2003 when he was apprehended in New Jersey for various crimes.** One of the biggest events he was involved with while working with the Secret Service as an informant was with “Operation Firewall.”

This was back in October of

2004 where **28 members of Shadowcrew.com, an illegal cyber organization, were arrested after Gonzalez – then under the name of “CumbaJohny” – led them to register in a federal-operated private VPN service sting operation.** However, it is now speculated now that he had **leaked information to other co-conspirators to prevent capture and prosecution – thereby circumventing his role as an ally to the Secret Service.**

Once the headlines about Operation Firewall subsided, Albert Gonzalez started operating under a different name, “Segvec”. **Together with 10 other men, Gonzalez hacked his way into the data-stores of major companies such as BJ’s Wholesale Club, Boston Market, Forever 21,**



### Credit Card Scams Are On The Rise...

**OfficeMax, Sports Authority, DSW, and TJ Maxx, the last of which shelled out \$130 million alone to cope with the aftermath.**

The 10 other men in Gonzalez's crew include two U.S. residents: Christopher Scott and Damon Patrick Toey; three are from Ukraine: Maksym Yastremski, Dzmitry Burak and Sergey Storchak; two from China: Hung-Ming Chiu and Zhi Zhi Wang; and the last two are from the countries Belarus and Estonia named Sergey Pavolvich and Aleksandr Suvorov respectively. The last remaining conspirator is known only as "Delpiero" and is still at large. Also cited in the indictment is a well known online seller of credit card and debit card information, Maksym Yastremski, who became Gonzalez's stateside hacker. Yastremski, otherwise known as "Maksik," is a Ukrainian but is now under the custody of Turkey. The indictment showed that Yastremski alone was able to earn at least \$11 million by selling credit information between 2004 and 2006.

According to court records, the breaches done by Gonzalez and the ten other criminals coincided with the New Jersey pre-trial court supervision, which means that while he was supposedly under the supervision of the New Jersey court system, Gonzalez was already working his way to even more advanced cyber crimes. **Stipulated in the government's conditions is the forfeiture of his belonging such as a condo in Miami, a 2006 BMW, and his Glock 27 firearm. He is also to pay fines in the amount of \$1,650,000 in cash.**

Gonzalez and the ten other men are now facing multiple lawsuits. The Boston indictment has charged Gonzalez for computer intrusion along with the other two United States residents, while the others were hit with trafficking of stolen data in San Diego.

There are other known cases of Secret Service informants, who while helping the United States government, have also been performing shady transactions on the side such as 2007's Brett Shannon Johnson who was responsible for the massive online scam involving identity theft in order to take advantage of the tax refund given out by the United States government during that time. Johnson, under the alias of "Gollumfun," was charged with prison sentence of a minimum of six years behind bars.

Indictment (PDF):

<http://www.usdoj.gov/usao/nj/press/press/files/pdf/files/GonzIndictment.pdf>