

IN THE UNITED STATES DISTRICT COURT FOR THE  
EASTERN DISTRICT OF VIRGINIA

Alexandria Division

UNITED STATES OF AMERICA	)	
	)	
v.	)	CRIMINAL NO. 1:11CR96
	)	
ROGELIO HACKETT, JR,	)	
	)	
Defendant.	)	

STATEMENT OF FACTS

The parties stipulate that the allegations in Counts One and Two of the Information and the following facts are true and correct, and that had the matter gone to trial the United States would have proven them beyond a reasonable doubt.

The United States Secret Service, as part of an on-going investigation to identify the Internet's largest on-line identity thieves, identified the defendant as a seller of credit card information in Internet Relay Chat ("IRC") chat rooms and on criminal carding forums, on-line discussion forums set up to promote identity theft. A federal search warrant executed on the defendant's residence on June 30, 2009 located 676,443 stolen credit card accounts on the defendant's computers and in his e-mail accounts. Credit card companies have identified tens of thousands of fraudulent charges on these accounts totaling \$ 36,624,815.52.

The defendant began hacking computers on the Internet starting in the late 1990s. His computer skills were noticed by others in IRC chat rooms and he was recruited to begin hacking for profit.

Beginning as early as 2002, the defendant began specifically to target computer databases that contained credit card information so that he could sell that information. The defendant

would hunt for vulnerabilities in SQL databases and exploit any security vulnerabilities he found in order to gain unauthorized access to such databases. He would then steal the credit card information stored in such databases.

For example, first in August 2007 and again on a later date, the defendant used his special skill in computer security in order to obtain unauthorized access to the computers of "Company One," an on-line ticketing services provider. Company One provides the ability to order and to pay for tickets ordered on-line for such clients as libraries, museums, theatres, performing arts centers, raceways, sporting teams, and festivals. The defendant stole a total of 359,661 individual access devices (i.e., credit card account information) from the computer systems of Company One. The defendant possessed many of these stolen access devices on his computers and storage media in his residence on June 30, 2009, the day the United States Secret Service executed a search warrant on that location.

In addition to hacking, the defendant also obtained stolen credit card information by purchasing it from others over the Internet. From May 2008 until June 30, 2009, the defendant bought stolen credit card information online from several different individuals he believed to be in the United States, Ukraine and Russia.

From at least as early as September 2004, the defendant was a member of various on-line carding forums, i.e., on-line discussion forums for the purpose of buying or selling stolen financial information. On one such carding forum, the defendant was a "Reviewed Vendor," a seller whose stolen financial information had been reviewed by someone assigned by the carding forum administrator.

From as early as 2002 until the defendant's residence was searched by the United States Secret Service on June 30, 2009, the defendant was routinely selling information for stolen credit

card accounts to people around the world, including at least the United States, Canada, Mexico, and the United Arab Emirates. From approximately 2002 through 2005, he was selling dozens of accounts on average per month, charging between \$20 and \$25 per account with track data and receiving at least \$200 and \$800 per month. Up until the time he was caught by the United States Secret Service, the defendant personally received more than \$70,000 from selling stolen credit card information.

In addition, from 2005 through 2007, the defendant and others with whom he conspired used stolen credit card information to purchase fraudulent Western Union orders. The defendant personally received at least \$30,000 and \$50,000 from fraudulent Western Union orders during this time period. During 2008, the defendant also would provide stolen credit cards to individuals who would purchase gift cards for him. The defendant would use the gift cards to purchase merchandise for himself, such as Louis Vuitton shoes costing more than \$450.

In or about May 2008, the defendant purchased a re-encoder, a device that allows a user to encode credit cards with the necessary information to make them work. In or about June 2008, the defendant purchased an embosser, a tipper, and a credit card printer, devices that allow a user to make credit cards that resemble legitimate ones. The defendant possessed this equipment in his residence on June 30, 2009, the day the United States Secret Service executed a search warrant on that location. The defendant also possessed over 100 counterfeit credit cards that he had made with this equipment.

On June 12, 2009, the defendant sold 25 counterfeit credit cards for \$630 to an undercover agent of the United States Secret Service in the Eastern District of Virginia.

On June 16, 2009, the defendant sold 15 counterfeit credit cards for \$550 to an undercover agent of the United States Secret Service in the Eastern District of Virginia.

In all, the defendant personally received over \$100,000 from his credit card fraud scheme. During the last several years, credit card fraud was the defendant's only source of income. The defendant used the proceeds of his illegal activities to purchase, among other items, a 2001 BMW X5.

Information concerning 650,259 individual credit card accounts was found on computers located in his residence on June 30, 2009. An additional 26,184 unique accounts not found on the defendant's computers was found in e-mail accounts belonging to the defendant.

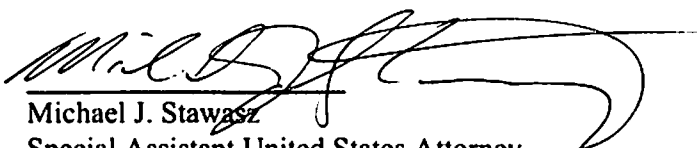
The credit card information that the defendant sold to others was used to commit far more fraud than the amounts the defendant personally received from his actions. Credit card companies report that they have received tens of thousands of reports of fraudulent charges throughout the country and around the world on the 676,443 accounts that the defendant had stole, bought and/or sold. Together, the fraudulent charges identified by credit card companies and relayed to the government totals \$ 36,624,815.52.

The defendant acknowledges that the foregoing statement of facts does not describe all of the defendant's conduct relating to the offense(s) charged in this case nor does it identify all of the persons with whom the defendant may have engaged in illegal activities. The defendant further acknowledges that he/she is obligated under his/her plea agreement to provide additional information about this case beyond that which is described in this statement of facts.


Respectfully submitted,

Neil H. MacBride  
United States Attorney


By:

  
Michael J. Stawasz  
Special Assistant United States Attorney

After consulting with my attorney and pursuant to the plea agreement entered into this day between the defendant, Rogelio Hackett, Jr. and the United States, I hereby stipulate that the above Statement of Facts is true and accurate, and that had the matter proceeded to trial, the United States would have proved the same beyond a reasonable doubt.

  
Rogelio Hackett, Jr.

I am Rogelio Hackett, Jr's attorney. I have carefully reviewed the above Statement of Facts with him. To my knowledge, his decision to stipulate to these facts is an informed and voluntary one.

  
Whitney Minter, Esquire  
Attorney for Rogelio Hackett, Jr.