COUNTERTERRORISM BLOG

WRITTEN STATEMENT OF
ANDREW R. COCHRAN
FOUNDER & CO-EDITOR
THE COUNTERTERRORISM BLOG

For the Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology Hearing
U.S. House Committee on Homeland Security

"Do the Payment Card Industry Data Standards Reduce Cybercrime?"

March 31, 2009

Chairmwoman Clarke, Ranking Member Lungren, and Members of the Committee, I appreciate the opportunity to submit a written statement on the subject of terrorists' use of credit cards for this important hearing. I am the Founder and Co-Editor of The Counterterrorism Blog, the first multi-expert Internet-based center dedicated solely to reporting and analyzing terrorist attacks and counter-terrorism policies. Now in its fifth year of operation, The Counterterrorism Blog is a highly respected source of objective information and analysis in the counter-terrorism community. Our Contriibuting Experts work in non-governmental organizations and private businesses worldwide, and include over 20 noted experts, including Evan Kohlmann, Douglas Farah, Dennis Lornel, Walid Phares, Animesh Roul. Farhana Ali, and Matthew Levitt. In addition to earning the plaudits of law enforcement, intellgence officials, Members of Congress, and the news media, our credibility is evidenced by the fact that Al Qaeda attacked us by name on Al-Ekhlaas, one of its central messaging forums, last April.[1] You can find us on the Internet at http://counterterrorismblog.org/, and you can e-mail me at ACochran@Gmail.com.

Our Contributing Experts have reported often on terrorists' use of stolen credit card information, and they speak often about the subject. On February 29, 2008, I chaired a special panel, "Meta-Terror: Terrorism and the Virtual World," with two Contributing Experts (Evan Kohlmann and Roderick Jones) and the Senior Vice President and Chief Technology Officer of VeriSign.[2]

[1] "Al Qaeda Officially Hates The Counterterrorism Blog," April 16, 2008, at http://counterterrorismblog.org/2008/04/al_qaeda_officially_hates_the.php.

[2] Complete transcript at http://counterterrorismblog.org/2008/03/event_transcript_and_related_1.php.

During that event, our discussion included how a senior Al Qaeda operative financed operations through the use of stolen credict card information. Dennis Lormel, who founded and ran the Terrorist Financing Operations Section at the FBI and investigated the financing of the 9-11 attacks, has several posts on terrorists' use of credit cards.[3] Matthew Levitt and Contributing Expert Michael Jacobson cited the use of credit card fraud to finance two deadly attacks in a *New Republic* article this year.[4] I invite the Committee to review the cited works in detail, and I will quote from and/or summarize their main points for the Committee's consideration as follows:

1. Credit cards are extremely vulnerable to fraud and are used extensively by terrorists. The internet not only serves as a learning tool for terrorists but also functions as a mechanism to steal credit card information through hacking, phishing and other means. In many instances, when terrorist operatives are apprehended, they have multiple identifications and credit cards in a variety of names in their possession.

2. The terrorists who executed the devastating 2004 Madrid train bombings, which killed almost 200 people, and who carried out the deadly July 7, 2005, attacks on the transportation system in London were self-financed, in part through credit card fraud.

3. Imam Samudra was a key operative of the Al-Qaeda linked terrorist group Jamaah Islamiah in Indonesia, and was the mastermind behind the Bali nightclub bombings in 2002 which killed over 200 people. While in prison in 2004, he wrote a jailhouse manifesto, with a chapter, entitled "Hacking, Why Not." In it, he urged fellow Muslim radicals to take holy war into cyberspace by attacking U.S. computers. Samudra described America's computer network as being vulnerable to hacking, credit card fraud and money laundering. Samudra discussed the process of scanning for websites vulnerable to hacking and then discussed the basics of online credit card fraud and money laundering. Interestingly, in 2004, Indonesian police asserted that Indonesia had more online credit card fraud than any country in the world.

4. Younes Tsouli, aka "Terrorist 007," and his two associates, Waseem Mughal and Tariq al-Daour, used computer viruses and stolen credit card accounts to set up a network of communication forums and web sites that hosted everything from tutorials on computer hacking and bomb making to videos of beheadings and suicide bombing attacks in Iraq. They raised funds through credit card information theft and fraud, which were used to support the communications, propaganda and recruitment for terrorists worldwide, as well as to purchase equipment for Jihadists in the field. One expert described their activities as "operating an online dating service for al-Qaeda." The three men pled guilty to inciting terrorist murder via the internet.

[3] "Terrorists and Credit Card Fraud…a Quiet Epidemic," February 29, 2009, at http://counterterrorismblog.org/2008/02/terrorists_and_credit_card_fra.php, and "Credit Cards and Terrorists," January 16, 2008, at http://counterterrorismblog.org/2008/01/credit_cards_and_terrorists.php .

[4] Summarized in "Drug Wars," Michael Jacobson, January 27, 2009, at http://counterterrorismblog.org/2009/01/drug_wars.php.

Set forth below is a snapshot of the extent of credit card information theft and fraud they were responsible for:

- Stolen credit card numbers and identities were used to buy web hosting services. At least 72 stolen credit card accounts were used to register more than 180 web site domains at 95 different web hosting companies in the U.S. and Europe.

- On one computer seized from al-Daour's apartment, some 37,000 stolen credit card numbers were found. Alongside each credit card record was other information on the identity theft victims, such as the account holder's address, date of birth, credit balances and limits.

- More than $3.5 million in fraudulent charges were made using credit card accounts stolen via online phishing scams and the distribution of "Trojan horses."

- The men purchased sophisticated equipment needed by jihadists in the field and other operational resources, including hundreds of prepaid cell phones, and more than 250 airline tickets using 110 different credit cards at 46 airlines and travel agencies.

- They laundered money through online gambling sites, using accounts set up with stolen credit card numbers and victims' identities. The trio conducted 350 transactions at 43 different online wagering sites, using more than 130 compromised credit card accounts.

The terrorists apparently obtained some stolen data through contacts with Russian-based criminal gangs, and they traded this information with criminal syndicates. In the 1990's, al Qaeda would steal a handbag to get one credit card to raise funds. Now they will just buy this data online and get thousands of credit card details. Once credit card information winds up in the hands of criminal syndicates, it can be easily transmitted to terrorists.

5. The Liberation Tigers of Tamil Eelam (LTTE), a.k.a. the "Tamil Tigers," use credit card fraud as an international means of financing terrorist activities. Four men, believed to be associated with the Tigers, were arrested this year in Toronto on charges of debit and credit card fraud for possessing numerous gift cards containing bank account and debit information from individuals in the United Kingdom. Further investigation found laptop computers and memory sticks containing bank information for thousands of U.K. bank customers. A massive credit and debit card fraud case in the U.K., involving up to 200 British gasoline stations, is apprently another Tamil Tigers operation. The alleged subjects obtained credit and debit card information at gasoline pumps through the use of skimming machines, with the loss was estimated to be as much as $72,000,000.

I look forward to reviewing the Committee's review into the effectiveness of the PCI standards to reduce data breaches, identity theft, and the potential funding of terrorism, and I stand ready to assist the Committee in that mission.