Carl Bulger presided.

PRESENTATION:

Michael R. Centrella, Special Agent, Washington Office, U.S. Secret Service, spoke to us on Attacking Identity Theft Together.

Mr. Centrella has been an agent of the Secret Service for eleven years, the first six in southern Manhattan on the Nigerian West African Task Force, four and a half years on the Presidential Protection Detail, and the last six months in the Washington area.

One of the Secret Services missions is to combat financial crimes. During his tenure on the Nigerian West African Task Force, they were successful in convicting one hundred major Nigerian offenders. This aided anti-terrorist efforts because the majority of proceeds of Nigerian scams go to Afghanistan and Pakistan Talibans and Al-Qaeda to purchase drugs.

Identity Theft is getting worse. Currently it afflicts one in every 20 people and amounts to $50 billion in losses. It is forecast to affect one in every five people per year. Approximately three members attending this meeting (3%) said that they had been victims of identity theft.

Thieves obtain your personal data by sophisticated and unsophisticated methods. They can steal your financial data from your mail box in the form of financial statements, pre-approved applications for credit cards, and convenience checks mailed with credit card statements. They can snatch your wallet or purse. They can go through your trash. They can break in to your home. They can "shoulder surf" (look over your shoulder while you use a computer, ATM, smartphone, or iPad. Or, employees can steal and sell the personal information of millions of customers. Countermeasures for these relatively unsophisticated crimes are fairly easy.

The more sophisticated methods of getting our personal data are tougher to combat. Even if you don't use Facebook or any of the other social interaction sites on the internet, your relatives may use them and inadvertently reveal your personal information. Criminals now use "social engineering" to get you to open a malicious e-mail or click on a link to a malicious website. For instance, within minutes of the announcement of Osama Bin Laden's assassination, criminal hackers were linking their websites to stories about his death. Unsuspecting people eager for more information clicked on links to those stories only to discover that malicious software had been downloaded to their computer.

Submitted by Barry Hammond, Secretary

We know about "phishing" employing websites emulating legitimate websites of banks, businesses, and organizations in an effort to obtain your logins and passwords and, ultimately, your personal financial or other information.

Mr. Centrella advised us to copy our passport, credit cards, and anything else that might be stolen when we travel abroad. Take the copies along to facilitate replacements.

We've been inundated with advice on how to combat identity theft. Most of the advice that Mr. Centrella gave us was old stuff to us, but it was an interesting review, especially when he inserted some of his personal experiences. As other speakers we've had, he abhors Facebook, Twitter, and the other social networking sites. When he warns his kids about them, they reply, "Oh, Dad! You're a COP, and you don't want us to have any fun!"

He said that McDonald's wants to allow customers to use EZPass to speed up payment of pickup orders. EZPass broadcasts your payment information and allows others to apply charges to your account.

Other vulnerable mechanisms: iPhones, iPods, iPads and other Wi-Fi and 3g or 4g devices, Blackberry signals, and RFIDs such as are present in some credit cards and in newer U.S. passports.

He suggested that we not put our photos on our credit or debit cards. That we not sign the back, instead write "Please request Photo ID". And get the free credit check from each of the three credit agencies each year so you can scan for fraudulent activity.

He warned that financial crimes are increasing because they tend to be High Reward – Low Risk.

He passed out a document prepared in 2005 and updated in 2008 by US-CERT (U.S. Computer Emergency Response Team) titled "Recognizing and Avoiding Email Scams". It and a lot of other advice is available at http://www.us-cert.gov/reading_room/ as downloadable .pdf files.

He also passed out three copies of a glossy Federal Trade Commission publication endorsed by the U.S. Department of Homeland Security and the U.S. Secret Service: Identity Crime – Take Charge! Fighting Back Against Identity Theft, June 2009. This is available at http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt04.shtm

Submitted by Barry Hammond, Secretary

Importantly, this tells you what do if you are a victim of identity theft, as well as giving advice how to avoid it.

Our speaker was:

Michael R. Centrella, Special Agent

U.S. Secret Service

Washington, DC Field Office

(202) 406-8800 (24 hrs/7 days)

Submitted by Barry Hammond, Secretary