



Shelby County Sheriff's Office
Shelby County, Alabama

Written Testimony of Clay Hammac
Criminal Investigator for the Shelby County Sheriff's Office

Hearing before The Committee on Financial Services

June 29, 2011

Chairman Bachus, Ranking Member Frank and distinguished Members of the Committee, thank you for the opportunity to testify before you today regarding the growing need for continued training and resources to be made available to local and state law enforcement at the National Computer Forensics Institute (NCFI).

The NCFI has proven to be a vital tool for local and state law enforcement agencies throughout this country. The analytical techniques and technical skill sets that are taught at the NCFI are invaluable to law enforcement. These skills are necessary for the successful investigation of growing crime trends throughout our nation.

Without question, electronic crimes make up the fastest growing crime trend in the United States and throughout the globe. According to a report from the US Attorney General's Office detailing a threat assessment of identity-related crime (U.S. Attorney General, 2010)¹, "With each passing year, identity theft, and the individuals and organizations behind it, become more complex and capable of rapid adaptation to changing circumstances..."

¹Identity-Related Crime: A Threat Assessment (November 2010)
<http://www.justice.gov/criminal/fraud/documents/reports/2010/11-01-10mass-market-fraud.pdf>

The absolute basic foundation of identity-related crime is the compromise of secured data held by private institutions, which typically is achieved by means of electronic intrusions. It is common knowledge within the law enforcement community that on any given day, there are thousands, if not tens of thousands, of individuals throughout the world hacking various point-of-sale systems within the United States, as well as compromising networks that hold valuable consumer information that will inevitably be used or sold to other criminal elements.

The growth of these crime trends has far outpaced the growth of the resources available to combat this activity. Fortunately, the NCFI provides local and state law enforcement agencies with the ability to confront the crimes as they affect the individual citizens of our communities and throughout our country.

The challenge for law enforcement

Technology has changed our lives and has also changed the way criminals do business in our country. Electronic crimes are becoming more popular due to the fact that criminals have discovered that in many small towns across our country, local law enforcement simply does not have the resources or capability to investigate such crimes. Sadly, these crimes do not rise to the level of a federal investigation, nor should they. With the investigation of complex electronic crimes resting with local and state law enforcement, the crimes often go unsolved.

Criminals exploit the lack of resources of local agencies to successfully investigate and prosecute these crimes. As a result, the criminals continue their crime spree, causing billions of dollars of financial loss each year (Federal Trade Commission, 2010)².

Electronic crimes are often faceless crimes. The traditional means of investigative work such as neighborhood canvassing, witness interviews, and processing physical evidence are all too often unnecessary and ineffective in the investigation of these crime types due to the fact that the criminal behind the act is typically one of only dozens involved, who are often discovered to belong to a complex organized ring of criminals who reside across several state jurisdictions.

Local and state law enforcement agencies also have observed an increase in the experimentation of committing electronic crimes among juveniles. One only needs to search Google or You Tube to receive tutorials on how to hack your neighbor's wireless network.

² Federal Trade Commission (February 2010)
<http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2009.pdf>

Needs of the Law Enforcement Community

It has sadly become far too common for law enforcement to encounter evidence of electronic crimes such as child pornography, fraud, embezzlement, espionage, cyberstalking and more recently, cyberbullying. Without specialized training and resources, these cases would certainly be impossible for local and state law enforcement to investigate and prosecute due to the anonymity of the Internet.

State and local law enforcement should not be left to face the technological challenges of the evolving industry of electronic crime without the necessary resources. With the assistance of the NCFI, men and women have received specialized training in complicated fields of data analysis and computer forensics and have taken the training back to their respective law enforcement agencies throughout the country, and they are now fighting on the front lines of the war against electronic crime.

This fight is not a fight that local law enforcement officers are willing to lose. The victims that we encounter on the state and local level are not always faceless corporations or financial institutions. The victims that we meet face to face are the ones who feel the pains of these crimes the most. These victims are retired steel workers who have lost nearly all of their savings due to fraud, the school teacher who had her credit card number compromised, the college student who has just discovered that someone has used his personal information during the last four years and has caused significant damage to his credit and reputation.

The victims that we encounter face to face look to us to solve their case, as they should. They look to law enforcement to win the fight against this crime. Yet, many small town law enforcement agencies across our country simply do not know how to investigate these crimes. The NCFI is addressing this challenge and equipping law enforcement with the tools needed to win this fight.

Shelby County Sheriff Chris Curry is one of the many law enforcement leaders in this country who has recognized the changing trend in crime within our communities across the United States. Sheriff Curry chose to utilize the NCFI to invest in his personnel and capitalize on the specialized training that is available at the NCFI.

In 2008, I was selected to attend the *Basic Investigation of Computer and Electronic Crimes Program (BICEP)*, followed by a *Network Intrusion Response Program (NITRO)* and the *Basic Computer Evidence Recovery Training (BCERT)*.

On the final day of my BCERT training, I was assigned to assist in the investigation of a quintuple homicide that was later linked to the Gulf Coast Drug Cartel and Los Zetas. Within less than 24 hours of completing my training at the NCFI, I was tasked with conducting forensic

examinations on more than a dozen computers and cell phones. The evidence and information gathered from the examinations proved to be vital in the successful arrests and pending prosecution of the hit men who were contracted to carry out the murders.

Prior to attending the NCFI, like many of my colleagues, I had a very basic understanding of computer skills. Three years later, I have completed more than 100 forensic examinations on computers and cell phones. Many of the examinations I have completed have been at the requests of neighboring law enforcement agencies. Such is the case for many graduates of the NCFI, thus alleviating the case loads for state crime labs as well as the Secret Service.

The results of the NCFI

It has been my personal observation that electronic and financial crimes far outnumber violent crimes. Though my training received at the NCFI has assisted me with the investigation and resultant arrests of violent crimes ranging from murder, kidnapping, and child pornography, it has proven equally vital in the investigation of financial crimes that range from embezzlement to organized Ponzi schemes.

Most recently, I was contacted by an employee of a nationally recognized insurance company. The employee made a simple complaint indicating that she believed her 401K account was electronically compromised. Utilizing the training I received from the NCFI, I was able to work with the third party company that is contracted to manage the employee retirement funds, as well as the Vice President of Security for the insurance company.

By tracing electronic routing numbers, bank account numbers, and identifying IP addresses, I was able to not only identify the offender that compromised the victim's retirement account, but I was able to illustrate that he did the same to four other employees, as well as embezzle nearly \$100,000 from the insurance company. The offender has since been arrested and indicted by a grand jury in two separate jurisdictions.

Another example of a recent complex financial crime that ended in the arrest of the offender was an organized Ponzi scheme in which the offender solicited investments from elderly members of local churches. The offender convinced the victims that the U.S. dollar would soon become worthless, and the federal government would seize control of their bank accounts.

Preying upon their fears, the offender accepted hundreds of thousands of dollars in investments from various victims in exchange for gold and silver. The offender never purchased the agreed amount of gold or silver. In fact, he used the funds for his own personal gain and simply pacified the victims with small amounts of precious metals.

During the investigation, the offender fled the country to avoid prosecution. He was later apprehended by Border Agents as he was attempting to walk across the Canadian border.

The foundation of this investigation was built upon the offender's electronic activity using online commodity markets to initiate trades that were less than what was agreed upon by the victims. Forensic examinations of the offender's computer and social media outlets further provided the evidence needed to seek an arrest and ensure the offender did not victimize anyone else.

Conclusion

The potential loss of these cases cannot be identified in dollars and cents. The money involved in these crimes makes up the retirement accounts that victims have invested in and depend on for their years to come. To the victims, the money involved was their livelihood and, in some cases, their entire savings.

The training offered at the NCFI is more than vital to the success of state and local law enforcement officers investigating a new wave of crime. Law enforcement is dedicated to not only responding to these reports of criminal activity but preventing these criminal acts. Such a task would be more than challenging without the tools and resources made available to us through the NCFI.

Chairman Bachus, Ranking Member Frank and distinguished Members of the Committee, this concludes my prepared statement. Thank you again for this opportunity to testify on behalf of local law enforcement officers. I will be pleased to answer any questions at this time.