HACKED OFF: HELPING LAW ENFORCEMENT PROTECT PRIVATE FINANCIAL INFORMATION

FIELD HEARING

BEFORE THE

COMMITTEE ON FINANCIAL SERVICES
U.S. HOUSE OF REPRESENTATIVES

ONE HUNDRED TWELFTH CONGRESS

FIRST SESSION

JUNE 29, 2011

Printed for the use of the Committee on Financial Services

Serial No. 112–43

U.S. GOVERNMENT PRINTING OFFICE
67–938 PDF WASHINGTON : 2011

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

HOUSE COMMITTEE ON FINANCIAL SERVICES

SPENCER BACHUS, Alabama, *Chairman*

JEB HENSARLING, Texas, *Vice Chairman*
PETER T. KING, New York
EDWARD R. ROYCE, California
FRANK D. LUCAS, Oklahoma
RON PAUL, Texas
DONALD A. MANZULLO, Illinois
WALTER B. JONES, North Carolina
JUDY BIGGERT, Illinois
GARY G. MILLER, California
SHELLEY MOORE CAPITO, West Virginia
SCOTT GARRETT, New Jersey
RANDY NEUGEBAUER, Texas
PATRICK T. McHENRY, North Carolina
JOHN CAMPBELL, California
MICHELE BACHMANN, Minnesota
THADDEUS G. McCOTTER, Michigan
KEVIN McCARTHY, California
STEVAN PEARCE, New Mexico
BILL POSEY, Florida
MICHAEL G. FITZPATRICK, Pennsylvania
LYNN A. WESTMORELAND, Georgia
BLAINE LUETKEMEYER, Missouri
BILL HUIZENGA, Michigan
SEAN P. DUFFY, Wisconsin
NAN A. S. HAYWORTH, New York
JAMES B. RENACCI, Ohio
ROBERT HURT, Virginia
ROBERT J. DOLD, Illinois
DAVID SCHWEIKERT, Arizona
MICHAEL G. GRIMM, New York
FRANCISCO “QUICO” CANSECO, Texas
STEVE STIVERS, Ohio
STEPHEN LEE FINCHER, Tennessee

BARNEY FRANK, Massachusetts, *Ranking Member*
MAXINE WATERS, California
CAROLYN B. MALONEY, New York
LUIS V. GUTIERREZ, Illinois
NYDIA M. VELÁZQUEZ, New York
MELVIN L. WATT, North Carolina
GARY L. ACKERMAN, New York
BRAD SHERMAN, California
GREGORY W. MEEKS, New York
MICHAEL E. CAPUANO, Massachusetts
RUBÉN HINOJOSA, Texas
WM. LACY CLAY, Missouri
CAROLYN McCARTHY, New York
JOE BACA, California
STEPHEN F. LYNCH, Massachusetts
BRAD MILLER, North Carolina
DAVID SCOTT, Georgia
AL GREEN, Texas
EMANUEL CLEAVER, Missouri
GWEN MOORE, Wisconsin
KEITH ELLISON, Minnesota
ED PERLMUTTER, Colorado
JOE DONNELLY, Indiana
ANDRÉ CARSON, Indiana
JAMES A. HIMES, Connecticut
GARY C. PETERS, Michigan
JOHN C. CARNEY, JR., Delaware

LARRY C. LAVENDER, *Chief of Staff*

CONTENTS

WITNESSES

WEDNESDAY, JUNE 29, 2011

APPENDIX

HACKED OFF: HELPING LAW ENFORCEMENT PROTECT PRIVATE FINANCIAL INFORMATION

Wednesday, June 29, 2011

U.S. House of Representatives,
Committee on Financial Services,
Washington, D.C.

The committee met, pursuant to notice, at 2:03 p.m., at the National Computer Forensics Institute, 2020 Valleydale Road, Suite 209, Hoover, Alabama, Hon. Spencer Bachus [chairman of the committee] presiding.

Members present: Representatives Bachus and Fincher.

Also present: Representative Rogers.

Chairman Bachus. Good afternoon. I see we have a group of witnesses seated. We also have several people in the audience who played an integral part in helping fund the project: Tony Petelos, the Mayor of Hoover; and Tommy Smith of the District Attorneys Association.

Randy, do you want to introduce some of them?

Mr. Hillman. Yes, sir. Yes, sir, Mr. Chairman. There are several elected DAs here. Tommy Smith is the district attorney from Tuscaloosa County. He's president of the association.

Chairman Bachus. Where is Tommy? There he is. Hey, Tommy.

Mr. Hillman. With your permission, Mr. Chairman, could I ask them to stand?

Chairman Bachus. Yes.

Mr. Hillman. Any elected district attorneys, would you stand, please?

Mr. Chairman, we have Chris McCool, the district attorney in Fayette, Lamar, and Pickens County; Brandon Falls, the DA in Jefferson County; Steve Marshall, the DA in Marshall County; and Tommy Smith, president of the association. Thank you.

Chairman Bachus. Do you have your investigators here?

Mr. Hillman. Yes, sir.

Chairman Bachus. And we have several members of the legislature. Would you stand up?

Mike, since you're the senior guy, why don't you introduce yourself? You are in front.

Mr. Hill. I'm Mike Hill, a State Representative from Shelby County.

Mr. Johnson. Wayne Johnson, District 22 Representative, from Huntsville.

Senator Blackwell. Slade Blackwell, Senator from Birmingham.

Chairman BACHUS. And Jan Williams in the back.

Mr. DEMARCO. And Paul DeMarco.

Chairman BACHUS. And Paul DeMarco, Representative DeMarco. So we appreciate—I thank everyone in the civil service and the District Attorneys Association. The State of Alabama was very supportive in their funding. I recognize the Shelby County Sheriff. Do you want to stand up and introduce yourself?

Do you have any other sheriffs? I'll let you introduce them.

Sheriff CURRY. Sir, I don't think there are any other sheriffs present.

Chairman BACHUS. Okay. We appreciate Shelby County's participation. I'm going to—I'm supposed to read this right now.

Without objection—actually, I can do it at the end of the hearing.

At this time, is there anybody else present who—the Secret Service—Gary, do you have anybody you want to introduce?

Mr. WARNER. If I may, yes, sir. We have the privilege of hosting a National Science Foundation group of researchers this summer, and several of our past student researchers from that team have joined us today, if they could stand briefly.

Allison Peck and Hugo and Megan were selected out of 116 applicants to come and study computer forensics at UAB this summer as a courtesy of the National Science Foundation. So we want to thank the National Science Foundation for them being with us.

Chairman BACHUS. Thank you. At this time, we're going to have opening statements from the witnesses. I'll introduce the witnesses.

I really want to kind of emphasize some things that some of you might not get into. I'm going to do it sort of from the standpoint of, I'm a former trial lawyer, which may be a dirty word.

But computer forensics is the process of extracting, analyzing, and preserving data. It is the process of getting it successfully introduced either at trial or into evidence or ready for evidence. It's a virtual gold mine of very vast, precise, and most importantly in a trial setting, our investigation of reliable and valuable information.

It's not a human being sitting on a witness stand with evidence that is imprecise or contradictory, subject to memory loss or prejudice or motive.

Two witnesses may testify about the same conversation. Each tells a different story, and each tells sometimes what they think is true.

Several witnesses might testify and still the picture is unclear and a gap exists. They tell a story about a steamboat up in New England that went around a bay, and it sank right in front of hundreds of people. And they said they were unable to determine what happened because there were too many witnesses.

And that is somewhat true. That's certainly not true with forensic evidence. It's altogether different.

Think about what's on your computer at home. It's thoroughly accurate. It's the most factual information available on what, when, and to whom something was said or when you did something, like in the Casey Anthony trial.

That information about chloroform was downloaded and, in fact, the technician who testified in the Casey Anthony trial on national TV was trained in this very center. And if you saw that testimony, the defense attorneys were unable to shake her. She was prepared for everything that they had to do. And also, I'm sure that she assisted the judge, or at least the prosecution, in the proper predicate to be laid so that there wouldn't be reversible error.

I know we have judges here today. We have a group of 26 judges from all around the Nation who are learning how to properly introduce evidence, how to rule on it so there won't be reversible error as they preside over a trial.

And I think law enforcement is very frustrated when a case goes up on appeal and it's turned back for a procedural technicality.

Not only emails and instant messages, but your personal and financial records are on a computer. Letters and memos, Web sites you have visited, it's all there.

I heard someone say this: It's like reading your mind in realtime, when you basically almost know what someone is thinking, what their motive is, and what's going on.

It can be highly revealing. And if you're engaged in criminal conduct—that's what this is all about—it's highly incriminating.

Last year—I think I have it in my written remarks—one of your software companies estimated that there's $1 trillion of software fraud worldwide. Here, at least $37 billion worth of losses.

Just this month, we have seen cyber security attacks and cyber attacks on Citigroup, on the Federal Reserve, and on the CIA.

So we're not talking about just criminal activity or financial crime, which was the motivation originally behind this center, but we're talking about actually espionage and people all over the world. And we'll get some terrific testimony.

I want to applaud the Secret Service. This institute was opened at a very—District Attorney Association—I think this was originally you working with the Secret Service, the District Attorneys of the United States. I think the sheriff's department and the police department were involved. You wanted a place to train people.

This is very complex, very detailed, very precise work, and it's very expensive, too, because of the software that is needed. It's always changing and evolving. But law enforcement and sheriffs and police departments didn't have the resources to combat these crimes.

And if you think about it, any time someone commits a crime, they're going to use an electronic device. It's almost impossible to do that without using cell phones.

We're not talking about just computers. We're talking about cell phones. We're talking about iPads. We're talking about BlackBerrys.

I know probably a year after this center opened, a detective who was trained here went back to a small town in Virginia and got out a computer that had been over in the corner for about 3 years, and they tried unsuccessfully to get anything out of it.

Using the software he was given here, he was able to pull it off the computer and successfully prosecuted a guy for sodomizing a 6-year-old child.

So it's pretty hard to put a figure on how valuable this center is. But, thanks to the Secret Service, thanks to the Alabama and National District Attorneys Office and the sheriff's department, thanks to the State legislature and the City of Hoover and Shelby County, and many other trials.

We have had at least one case where someone was being investigated for a murder, and they were cleared, forensic evidence cleared them. So you had someone who may have been charged and was able to prove their innocence.

The witnesses today are going to tell you about some of the details of cyber crime, which is now, I guess, the fastest growing crime in America. And none of us are safe.

Of course, I think very seldom is there not a person who is either—has been hacked or will be hacked, their computer.

I don't know whether it was my computer or someone else's that was hacked, but I have had charges on my credit card, and I was notified the very next day that it had, in fact, happened. And it's kind of funny when you go on there—or not funny, but you go in and you actually see those charges.

But with that, I would like to introduce and to turn it over to Mike Rogers, one of the senior members of the Homeland Security Committee, to make an opening statement.

Mr. ROGERS. I just wanted to thank Spencer for calling this hearing. As he mentioned, I was on the Homeland Security Committee before it was a standing committee. It was a select committee before 9/11, and we recognize the real threat of cyber security authorities have for our Nation. The Department has been working aggressively to that end.

I'm very pleased with the presence of this entity, this site in Alabama. Folks don't think about this kind of cutting-edge technology here in Alabama, but it is here, and we're very proud of it.

Randy and his folks have done a good job in the outset of keeping me apprised of what they have been doing. I have been very supportive, and I know this will be very critical in continuing to protect our Nation.

A lot of people think about the Department and the FBI and the Secret Service being on the cutting edge, but the fact is, we can't do it without local law enforcement. These partnerships that we have in local communities are critical in identifying these cells, the people who are problems, the threats, and monitoring activity.

And I have been amazed through the work of this entity, like Spencer said, how much of our lives is on a gadget, whether it's a computer or BlackBerry or cell phone.

And even when it comes to small drug deals, there is a cell phone involved. This is very critical technology, and I'm very supportive of it and look forward to the testimony we have here today.

Like Spencer, I had Secret Service knock on my door one day and tell me that someone had attempted to steal my identity, as well as the identities of about 20 other Members of Congress. Fortunately, they didn't succeed, but it could be anybody. You never know who they are. Thank you. We look forward to hearing the testimony and asking a few questions.

Chairman BACHUS. Thank you. And actually, I asked Gary Warner to introduce those people, but you're with UAB.

That reminds me, Gary Warner actually was one of the people who called and told me that my congressional site had been hacked.

So anyway, let me introduce our witnesses.

Oh, I'm sorry. Steve is one of my good friends and one of the newly elected Republicans to the Congress and to the Financial Services Committee. In fact, he is the newest member of the Financial Services Committee. Steve Fincher. And—

Mr. FINCHER. Thank you, Mr. Chairman.

Chairman BACHUS. I take back everything I said about your tie.

Mr. FINCHER. Well, Mr. Chairman, I'm wearing my orange tie today for Auburn. It's not Tennessee. It's Auburn. My middle son is a big Auburn fan. I was able to bring him down last year to homecoming and it is just a great, great college, a great place.

I was listening to the chairman and Congressman Rogers talking about hacking into our credit cards. And I thought one day that mine had been hacked into. Come to find out, my wife had been shopping. Seriously, that's what I thought it was.

So it's an honor to be here with you guys today. We can't say enough about local, State, and Federal law enforcement and what you guys do in the legal system. It's not if we're going to have an attack; it's when. We're either moving forwards or backwards.

And it's an honor to be able to serve in the leadership of someone like Chairman Bachus because he gets it.

I'm from Tennessee and I'm just a common sense guy. My background is a seven-generation cotton farmer. We need to make sure that our priorities are in the right order. And a lot of times, they're not.

But you guys are offering a great service to this country, and you're going to stand in the gap when we have another attack and when they attack us in this way, because as many of us know, this could shut our country down if the right people get the right information and go about it the right way.

So I am very, very interested in hearing what the panel has to say today, and it's good to be back in the State of Alabama, one of our bordering States.

With that, I will turn it back over to Chairman Bachus.

Chairman BACHUS. I'm going to introduce the witnesses at this time. I just noticed that Joe Borg is here, the Alabama Securities Commissioner. Joe, would you stand up?

Randy, did you introduce everyone in the unit? And how about the Secret Service Commission? Do have anybody you want to introduce? I know you have several people here.

Mr. HILLMAN. I do, actually.

Chairman BACHUS. In fact, it was testified to before some of our security members, which was incredible.

Mr. HILLMAN. I do, Mr. Chairman. Thank you. I would like to recognize several of our people who are here today: Special Agent in Charge Ken Jenkins, who is in charge of our Criminal Investigative Division, which again is our sort of nexus of nationwide oversight; Deputy Special Agent in Charge Pablo Martinez, whom I think you have met before; and Special Agent in Charge Roy Sexton of the Birmingham office, which is responsible for the entire State of Alabama and has a lot of interaction obviously with this institute among others that are here.

Chairman BACHUS. Thank you. Will you gentlemen stand up? Thanks.

Thank you. And let me say this: When I was talking to different people who played a role, obviously the bigger role is the Secret Service. The Secret Service is the entity that runs this center—along with the cooperation of the district attorneys—and makes their expertise available. So we can't thank you enough, I think, for the excellent job you do.

And this obviously goes beyond counterfeiting, and it is a tremendous challenge. So thank you very much.

Spencer Collier is the Alabama Homeland Security Director. Thank you.

Mr. HILLMAN. U.S. Attorney Joyce Vance is here.

Chairman BACHUS. Okay. I had no idea. Would you please stand up?

Ms. VANCE. I am happy to be here with you.

Chairman BACHUS. Thank you very much. Congratulations on your appointment.

Ms. VANCE. Thank you.

Chairman BACHUS. Her father is Judge Vance, who is actually a sitting judge who was attacked and wounded by a bomb.

But anyway, we'll go ahead now and introduce our witnesses. Gary Warner is director of research in computer forensics at the University of Alabama at Birmingham where he teaches in the computer and information science and justice science departments with more than 20 years of IT experience.

He previously served on the national boards of the FBI InfraGard program and the DHS Energy ISAC. His lab works closely with the Birmingham FBI cyber crimes task force and the Birmingham USSS electronic crimes task force with whom he shares his research on spam, malware, investigating on-line crime, and—I guess that's phishing. How do you—

Mr. WARNER. Phishing. It's tricky with the "P-H."

Chairman BACHUS. Thank you.

Randy Hillman is the executive director of the Alabama District Attorneys Association of the State Office for Prosecution Services, a position he has held since January 2002. Prior to this, he was chief assistant DA for the Shelby County District Attorney's Office.

And Robbie is here. Were you introduced, Robbie?

Mr. OWENS. I was left out as usual.

Mr. HILLMAN. Thank you, Mr. Chairman. I appreciate that.

Robbie Owens is the district attorney from Shelby County, which is where this facility is located.

Chairman BACHUS. Thank you.

During Mr. Hilman's tenure, he led trial counsel in seven capital murder prosecutions where the defendant received the death penalty or life without parole, many of them tried before my former partner, and he tried numerous other high-profile cases, including the road rage murder.

Randy is a member of the Alabama Bar Association, Shelby County Bar Association. He's on the Board of Trustees at the University of West Alabama and the Board of Directors for Owens House, which is a child advocacy center.

He was really a moving force in visualizing the need for the National Computer Forensic Institute, and working with the Secret Service in partnership to bring it here. It wouldn't have happened without Randy and his association. Or it may have cost a whole lot—

I don't know whether you know this, in the crowd, but the City of Hoover—you can see what a beautiful facility this is—donated this at no charge for 7 years rent free.

One of the sites they were considering was up at Aniston Army Depot, where they were going to spend several million dollars to renovate it.

Mr. ROGERS. Thank you for reminding everybody we lost.

Chairman BACHUS. I actually always wanted to renovate something and—it was one of the few things that hadn't gone to West Virginia. You can actually get here from there.

But Clay Hammac is a 7-year veteran of the Shelby County Sheriff's office, currently assigned as a criminal investigator specializing in financial and electronic crimes. He's a 2008 graduate of the National Computer Forensic Institute and has utilized his skills and training received here to investigate crimes ranging from the typical on homicide to organized financial crime rings. And that was the case off 280 there?

Mr. HAMMAC. Yes, sir. That's right.

Chairman BACHUS. That was one of the most heinous crimes you can imagine.

Mr. Hammac holds a degree in finance from the University of South Alabama, and an MBA from Regis University in Denver.

And finally, I guess the star witness is A.T. Smith, Assistant Director of the United States Secret Service. We're honored to have you here in Hoover.

A.T. Smith is from Greenville, South Carolina, and was appointed Assistant Director of the Office of Investigations in October 2010. In this capacity, he develops and implements policy for all Secret Service criminal investigations pertaining to counterfeit currency and financial crimes and electronic crimes.

Mr. Smith is responsible for oversight of the Secret Service Criminal Investigative Division, Forensic Service Division, Investigative Support Division, Asset and Forfeiture Division, International Programs Division, and over 3,000 personnel assigned to 140 domestic and 22 international offices in 6 continents. Some of those are pretty unfriendly territories.

So we welcome our witnesses. Do any of you want to suggest an order we go in? Why don't you go first, Mr. Smith, since you are here as our guest?

STATEMENT OF ALVIN T. SMITH, ASSISTANT DIRECTOR, OFFICE OF INVESTIGATIONS, UNITED STATES SECRET SERVICE

Mr. SMITH. Thank you, and good afternoon, Chairman Bachus and members of the committee.

If I might, just at the outset, let me say that with regard to what you said about the Secret Service being integral in the forming of this institute, that is true.

But we are equal among partners. And we are all in this together. I can assure you that no one has worked harder, again as you pointed out, than Randy Hillman to design and coordinate and actually get this facility to where it is today. So I want to publicly thank him as well.

Thank you for the opportunity to testify on the emerging threat that cyber criminals pose to both personal and business finances and to financial institutions.

On February 1, 2010, the Department of Homeland Security delivered the quadrennial Homeland Security Review, which established a unified strategic framework for Homeland Security missions and goals and underscored the need for a safe and secure cyberspace.

In order to be successful in this mission, we have to disrupt criminal organizations and other malicious hackers engaged in high consequence or widescale cyber crime.

In this arena, the Secret Service has been leading the Department's effort for some time. As the original guardian of the Nation's financial payment systems, the Secret Service has a long history of protecting American consumers, industries, and financial institutions.

Over the past decade, Secret Service investigations have revealed a significant increase in the quantity and complexity of cyber crime cases. Broader access to advanced computer technologies and the widespread use of the Internet has fostered the proliferation of computer-related crimes targeting our Nation's financial infrastructure.

Current trends show an increase in network intrusions, hacking attacks, malicious software, and account takeovers which result in data breaches that affect every sector of the American economy.

As a result of this increase and in line with the Department's focus of creating a safer cyber environment, the Secret Service developed a multifaceted approach to combat cyber crime by expanding our electronic crimes special agent program, expanding our network of Electronic Crimes Task Forces, creating a cyber intelligence session, expanding our presence overseas, performing partnerships with academic institutions, focusing on cyber security, and working with the DHS to establish the National Computer Forensic Institute.

The Secret Service partnerships with State and local law enforcement remain at the very core of our approach and are reflected in our task force model and through the work conducted here at the NCFI.

The 31 Electronic Crimes Task Forces (ECTFs) that the Secret Service established domestically and abroad exemplify the Secret Service's commitment to sharing information and to best practices.

Membership in these ECTFs include more that 4,000 private sector partners; nearly 2,500 international, Federal, State, and local law enforcement officials; and more than 350 academic partners.

Based on this model, the Secret Service has been responsible for the arrest of numerous transnational cyber criminals who were responsible for some of the largest network intrusion cases ever prosecuted in the United States.

These intrusions resulted in the theft of hundreds of millions of account numbers and a financial loss of approximately $600 million to the financial and retail institutions nationwide directly impacting the lives of many American citizens.

Recognizing that cyber crime is not just a Federal problem, the Secret Service partnered with the National Protection and Programs Director of DHS, the Alabama District Attorneys Association, the State of Alabama, and the City of Hoover to create a center where State and local law enforcement officials, prosecutors, and judges could be trained on cyber-related crimes.

I am proud to say that since its establishment, 644 State and local law enforcement officials, 216 prosecutors, and 72 judges representing over 300 agencies from all 50 States as well as 2 U.S. Territories have received training from the Secret Service here at the NCFI.

In concert with our Federal, State, and local law enforcement partners, the Secret Service will continue to play a critical role in preventing, protecting, and investigating all forms of cyber crime.

Chairman Bachus and distinguished members of the committee, this concludes my prepared remarks, and I will be happy to answer any questions that you may have.

[The prepared statement of Assistant Director Smith can be found on page 43 of the appendix.]

Chairman BACHUS. Thank you. Mr. Hillman?

STATEMENT OF RANDALL I. HILLMAN, EXECUTIVE DIRECTOR, ALABAMA DISTRICT ATTORNEYS ASSOCIATION

Mr. HILLMAN. Thank you, Mr. Chairman. Chairman Bachus, Congressman Fincher, Congressman Rogers, Governor Bentley, honorable members of the Alabama legislature, other guests, and our respected colleagues in law enforcement, thank you for the opportunity to address this committee today.

In the last 25 years, the criminal justice community has witnessed two watershed events with respect to criminal law. The first is the advent of DNA evidence. The second, and the reason that we're here today, is the creation and proliferation of digital evidence and cyber crime.

In my current position as executive director of the Alabama District Attorneys Association, it is my daily job to analyze and attempt to meet the needs of law enforcement and prosecutors. Without question, the need for digital evidence training is one of our most pressing.

The media work escalation of digital evidence can be compared to a tidal wave looming over the criminal justice community. This type of evidence is present in the majority of all cases, whether it is identity theft, phishing, child pornography, murder or any other crime.

We have very quickly moved from just blood and guts to megabytes and megapixels. The question is, do we as law enforcement agents and prosecutors have the means to gather that evidence? And the answer in most cases is a resounding no, we do not.

Gentlemen, you know better than most anyone that we cannot stick our proverbial heads in the sand. We must endeavor to be ahead of the curve. We must be ahead of the criminals who would prey on our family's financial security. This effort starts here at home.

When I was a child, the bank was a brick building in the center of town that you walked into to deposit a check or to withdraw money.

Today, we can access our virtual bank nearly anywhere. This convenience, although desirable, makes us extremely vulnerable to criminals.

I will submit to you that not one individual in this room has not had their personal data or financial holdings compromised in some way due to a surreptitious intrusion by a cyber criminal.

We are not immune and our children are not immune either. They are by definition prime targets for identity thieves because they have identifiers. They have information that is considered pristine because they generally will not discover that their identity has been compromised for several years. This gives the criminal a very long time to use our identity fraudulently.

We are bringing forth a crop of young adults who will exist entirely on technology-based banking and commerce. Today, our kids and young adults have credit cards, PayPal accounts, PlayStation credit accounts, Wii accounts, and Apple APP accounts.

Each of these areas are fertile grounds for a cyber criminal. And once one of these accounts is compromised, who we will call? More often than not, it will be your local police department or your local prosecutor who will then be asked to investigate and prosecute these bad guys.

Additionally, at the opening of this facility in 2007, Chairman Bachus stated that terrorists such as Osama Bin Laden were using technology and the Internet to fund and to manage their worldwide terrorist networks most often by identity theft, bank fraud, and phishing.

Recently, his comments were proven true after the capture and killing of Bin Laden. Bin Laden had in his possession hundreds of computer disks and digital devices containing priceless evidence that will be used to understand terrorist networks and ultimately help eliminate them.

Similarly, domestic and international terrorists and common criminals fund their criminal enterprises through the use of cyber crime and digital devices. They do this by compromising banking systems through network intrusion and stolen identities. This not only cripples our banking industry and financial institutions, but it devastates our citizens.

Some would say this is strictly a Federal matter, Mr. Chairman, but I wholeheartedly disagree. The State and local law enforcement in this country tries over 95 percent of the criminal cases. Those officers on the street are the first responders and they are absolutely critical to building an identity theft or network intrusion case and will, in the end, provide the key evidence that will convict criminals and provide restitution for victims.

Members of this committee, it's imperative that all law enforcement agents and prosecutors be given the ability to protect your constituents. It is both shocking and tragic that law enforcement is ill equipped and trained to respond to a digital crime scene.

I submit to you that the only way we can change this is by greatly expanding training for law enforcement and prosecutors and by providing them with the equipment they need to do their jobs properly.

Unless and until we do these things, thieves, scammers, pedophiles, and other criminals will continue to go unpunished because they know that we simply do not have the ability to reach out and catch them.

Chairman Bachus, Senator Shelby, Alabama District Attorneys and my staff at the ADAA set out to address this issue some years ago. We experienced the lack of quality computer forensics training firsthand. Our trials in attempting to find trained law enforcement agents and prosecutors to staff our own computer forensics labs were the catalyst.

Because no one entity made it their mission to train law enforcement, prosecutors, and trial judges in digital evidence, we were left in a very difficult position of staffing these labs. This facility that you are at now, the National Computer Forensics Institute, is a direct result of this need and the unprecedented cooperation of all levels of government, from the highest Federal agencies to the smallest local governments.

This facility focuses on all computer-related crimes with an emphasis on financial crimes, and more importantly, is taught by true investigators who have been and are now in the field each day. They understand and teach the curriculum from a law enforcement perspective, not that of an academician or a layman.

I witness each and every day the inherent value of quality digital evidence training and education here, and I know that the graduates from this facility have both solved thousands of criminal cases and have prevented many others from being committed.

In closing, I would like to thank you for being here, Mr. Chairman and members of this committee. Your presence is both a sign and a promise that you are committed to a unified front against cyber criminals.

Furthermore, I respectfully challenge you to join me and my colleagues in law enforcement to ensure that training facilities like NCFI that train authorities to investigate, prosecute, and even prevent cyber crimes and other crimes remain as one of our top priorities.

Thank you, Mr. Chairman.

[The prepared statement of Mr. Hillman can be found on page 39 of the appendix.]

Chairman BACHUS. Thank you. And, Gary, before we go to you, I notice that one of our Supreme Court judges is here, Michael Joiner. Would you stand up, Mike?

Judge JOINER. Court of Criminal Appeals.

Chairman BACHUS. Court of Criminal Appeals. I appreciate you being here. And did you try the four criminals that we were talking about earlier?

Judge JOINER. I tried many of the ones you talked about earlier.

Chairman BACHUS. Okay. We appreciate you. Are there any other judges or anyone else that I should have introduced?

I didn't have a list. A lot of times I have a list, but I didn't get one.

Mr. HILLMAN. Mr. Chairman, former Congressman Bob McEwen is with us today.

Chairman BACHUS. Oh, wow! Bob, it is good to see you. Thank you. We're honored to have everyone.

Do we have any other law enforcement officers that we have not recognized? Would you stand up? Thank you. I appreciate you all being here.

Chris Curry of Birmingham. So—I guess he's deputy chief; is that—

Mr. CURRY. Chief deputy, yes, sir.

Chairman BACHUS. Chief deputy. I want to welcome you.

With that, Mr. Warner.

STATEMENT OF GARY WARNER, DIRECTOR OF RESEARCH IN COMPUTER FORENSICS, THE UNIVERSITY OF ALABAMA BIRMINGHAM

Mr. WARNER. Thank you, Mr. Chairman. Mr. Chairman and members of the committee, I'm very happy to be before you today at this hearing. I think this hearing is a sign of your wisdom and your leadership in the financial services area. I'm very glad that you chose to have it here in Alabama because there are some very neat things happening here at the National Computer Forensics Institute and around the State. So we thank you for that.

Some of you may wonder what the University has to do with law enforcement. We feel like we're contributing to the cyber crime efforts in three main areas.

First, we're training the next generation of cyber crime investigators. Because we have a partnership with our computer science and our justice science programs, we feel like we're offering a very unique graduate, someone who comes with both a formal understanding of the justice process and a computer science background to go with it.

The second area is that we're providing through my research lab training and tools and techniques for fighting cyber crime. Some of these datasets that we work with, there are a million computers involved in a single live net. And you need some high-powered computer science if you're going to be able to analyze those sorts of datasets.

The third area that we're working with is in the area of outreach and public education. We call it actually reducing the victim pool.

The more we can identify outstanding threats that are currently emerging, the more we can protect people by sharing information with them in the media and in speaking in specialty conferences. We don't just do training for computer scientists; we also do training for health care information and workers for educators and other organizations.

I think it's important that the committee understand that this is the fastest growing category of crime.

If we look back to the year 2000, in 2000, there were only 360 million people on the Internet. And almost all of them were in the United States.

That year, e-commerce really took off for the first time. There were $5 billion worth of transactions that year.

If we go forward a decade to 2010, we're sitting at $164 billion of online commerce last year, a 3200 percent increase. We now have 2 billion users of the Internet, and only 13 percent of them are in the United States.

We're now dealing with a situation where the United States is the holder of most of the wealth that's accessible to the Internet, and yet 87 percent of the Internet users live in countries, many with shattered economies, which would like a piece of that wealth.

One of the areas that we're struggling with is the lack of computer science that has been applied to this area. Not only has the criminal element grown on the Internet, as the economy has grown, we're also dealing with very advanced sophisticated computer criminals.

These people are getting advanced computer science degrees, Ph.D.s in computer science and economics, and then are unable to find a job in their home economies. And they're taking those technology skills and working with the Russian Mafia and other organizations to come after our money.

Law enforcement has not had a similar increase in focus in high-tech crime fighting. That's one of the things we're contributing from the University.

I'm also very concerned about the lack of complaints. When we look at the Federal Trade Commission's consumer sentinel report, last year they identified 1.3 million victims of fraud and identity theft.

Unfortunately, all of the best surveys were saying there were closer to a million victims of identity theft. Where do those other 9.7 million complaints go?

We have trained our consumers that to be a victim of a cyber crime is not something that you should engage law enforcement on. You should call your bank. You should call your credit card company.

Until we have access to the truth about those complaints, until we know how many victims of cyber crime there are and until we have a good way of gathering that evidence in a way that has meaning, not just I lost some money but answering particular questions, we aren't going to be able to do intelligence-based policing of the Internet.

That's one of the places that we have also established a partnership that you may not have heard of. It's called Operation Swordphish.

Randy Hillman's office and my lab at UAB have been working with the Department of Prosecutorial Services and the Alabama District Attorneys Association and the Department of Public Safety in Alabama to try to do something about this.

We have developed a Web site and a PSA campaign to attract complaints from Alabama citizens who may have been victims of cyber crime and are unaware that they ought to be reporting these things to law enforcement.

Our Web site will gather those complaints. Our students will help to triage that data and combine it with the evidence that we have in our databases so that we can make qualified referrals to law enforcement.

We think that this is one of the important things we have to do to move forward, and we're looking forward to answering any other questions you may have about these efforts.

[The prepared statement of Mr. Warner can be found on page 50 of the appendix.]

STATEMENT OF DOUGLAS "CLAY" HAMMAC, CRIMINAL INVESTIGATOR, SHELBY COUNTY SHERIFF'S OFFICE, SHELBY COUNTY, ALABAMA

Mr. HAMMAC. Chairman Bachus and distinguished members of this community, 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.

It has become unfortunately far too common for law enforcement to encounter evidence of electronic crimes such as fraud, embezzlement, and even espionage.

Without specialized training and resources, these cases would certainly be impossible for local and State agencies to investigate and prosecute due to the anonymity of the Internet.

Without question, electronic and financial crimes are the fastest growing crime trends in the United States and throughout the globe.

With each passing year, identity theft of individuals and organizations behind it become more complex and capable of rapid adaptation due to changing circumstances.

The foundation of identity-related crime is the compromise of secured data held by private institutions, which typically is achieved by means of electronic intrusions. And it's 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 here within the United States as well as compromising networks that hold valuable consumer information that will inevitably be used by or sold to other criminal elements.

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

Electronic crimes are becoming more popular due to the fact that the criminals have discovered that in many small towns across our country, local law enforcement simply does not have the resources or the capability to investigate such crimes.

As a result, the criminals exploit the lack of resources, and complex electronic and financial crimes are often unsolved.

These crimes are difficult to solve due to the fact that 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 with these type of crimes.

With the assistance of the NCFI, law enforcement men and women across this country have received specialized training in complicated fields of data analysis and computer forensics.

They have taken this training back to their respective agencies throughout the country, and they are now fighting on the front lines in this war against electronic crime.

Shelby County Sheriff Chris Curry is one of the many law enforcement leaders in this country who has recognized the change in crime trends within our communities and the United States.

Sheriff Curry chose to utilize the NCFI to invest in his personnel and capitalize on this specialized training.

Prior to attending the NCFI, I, like many of my colleagues, 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 have been at the request of neighboring law enforcement agencies, as is the case for many graduates of NCFI, thus alleviating the case loads for State crime labs as well as the Secret Service.

And though my training at the NCFI has assisted me in the investigation and resulting arrests of violent crimes such as the quintuple homicide I was requested to assist with less than 24 hours after completing my training here, it has proven equally vital in the investigation of financial crimes that range from embezzlement to organized crime scenes.

As a very brief example, I was recently contacted by an employee of a nationally recognized insurance company. The employee made a simple complaint indicating that she believed her 401(k) account was electronically compromised.

Utilizing the training that I received from the NCFI, I was able to trace electronic routing numbers, bank account numbers, and identifying IP addresses. Not only did I identify the offender that compromised the data entry of the retirement account, but also illustrated that he had done the same to 4 other employees as well as embezzled nearly $100,000 from the insurance company.

That offender has since been arrested and indicted by a grand jury in two separate jurisdictions. The potential loss in this case cannot be identified by dollars and cents. The money involved in this case makes up the retirement accounts that the victims have invested in and depend on for many years to come.

Law enforcement is dedicated to not only responding to these reports of criminal activity but also preventing these criminal acts. And such a task would be more than challenging without the tools and resources made available to us through the NCFI.

Chairman Bachus and distinguished members of this committee, this concludes my prepared statement. Thank you for this opportunity to testify on behalf of local law enforcement officers, and I'll be pleased to answer any questions that you have.

[The prepared statement of Mr. Hammac can be found on page 34 of the appendix.]

Chairman BACHUS. Congressman Rogers?

Mr. ROGERS. As you heard, Chairman Bachus and Congressman Fincher are with the Financial Services Committee, so they're going to be much more focused, I'm sure, on the financial crime than I am. I'm more focused on threats to our homeland than cyber security stuff.

My concern is there, so I'm going to make that the focus of my questions.

Mr. Smith, you talked about a number of people who received their training here, a relatively small number when you think about it. What is the number that you think should be annually having access to this training?

Mr. SMITH. As I said, we have trained a significant number of people. And quite frankly, the positive of that is—which I didn't elaborate on as much—that we used this as a force multiplier, because what we are able to accomplish here through training is literally putting a mini crime lab, if you will, in every one of the locations that those individuals represent.

When they go back to the field, they are able to take the knowledge and expertise that they gain here and apply that not only in their department there locally, but as you heard Mr. Hammac say, from other departments regionally.

And I think we have done a very good job in terms of spreading the wealth, if you will. There has been pretty equal representation from all of the States across the country.

Having said that, we, as you saw in my prepared remarks, operate at about 25 percent here. We understand, like certainly members of the committee do, that budget issues are always a concern. But quite frankly, we could always do more, if that opportunity comes our way.

It would be hard for me to put an exact number on that because again, it is such a benefit for us to approach this, as I have said, from a force multiplier standpoint.

So in terms of actual numbers, I'm sure that's something that we could get for you after we delve a little further, if need be. I think that would be the best way to answer it. We could always use a little more, but certainly I think we're able to accomplish a lot with what we are able to have and to do.

Mr. ROGERS. Thank you. Mr. Hillman?

Mr. HILLMAN. Congressman, right now we are running at this facility somewhere around 25 percent capacity. We could—we are putting, give or take, 400 people per year in this facility. The capacity is 1,600. And we have—

Mr. ROGERS. This is a big facility. Just because you have the capacity doesn't mean it's needed. That's what I'm after.

Mr. HILLMAN. Yes, sir.

Mr. ROGERS. How many people would like to get in here but can't because you just don't have the funding to meet that need and it's really inhibiting your ability to pursue leads and crimes and threats that are out there that need pursuing? That's what I'm asking.

Mr. HILLMAN. Congressman, we are running anywhere from 8 to 10 to 12 applicants per spot right now trying to get in here.

Mr. ROGERS. How is that applicant selected and how are they—what's the criteria for their approval?

Mr. HILLMAN. The Secret Service, that's the State and local law enforcement candidates through their local field offices. There are special agents in charge—in charge of gathering those names and then they select those candidates.

The Alabama District Attorneys Association, that's the candidates for prosecutors and judges throughout the country. There's a lot of give and take on both sides. There are lots of people from different jurisdictions who need to come here that we might not know about that the Secret Service does and vice versa.

Mr. ROGERS. Mr. Smith, how many of these folks are backed up and can't get in here because of space?

Mr. SMITH. Again, as Mr. Hillman said, I would say on average with every class, we turn away about 60 percent of the candidates who apply.

Mr. ROGERS. What's the criteria of the ones that you do approve?

Mr. SMITH. Again, like Mr. Hillman said, it's almost a pyramid. The local agencies, sheriffs' offices, and police departments make it known to our special agents in charge that our—within our 45 field offices around the country that they have a candidate that they would like to put forward and are interested in having someone attend this training.

From there, that special agent in charge will submit the names and the biographical information of those individuals, and then it is actually looked at again at our headquarters level to do the things that I mentioned a minute ago, to make sure that we're disbursed equally across the country, that those areas which have a very high incidence of this sort of crime are given some priority.

So it's really a lot of things that go into the equation. We try to make sure at the end of the day that the back-and-forth multiplier, a term that I use, that we're putting the right number of people in the right places based on the availability that we have and, again, trying to be equal across-the-board throughout the entire country.

Mr. ROGERS. As you heard Randy Hillman state in his opening statement, when Bin Laden was killed, we captured a lot of computer data that has been a real wealth of information for us in the fight on terror. That has been the case throughout the Middle East when we have killed leaders in the Al-Qaeda movement.

What a lot of people may not understand is that we have a lot of those cells here, folks here who are collaborating. The best example, as most of you are aware of, is the young man from Mobile who graduated from high school and is over there fighting, the same thing, using the Internet.

How much of the information sent to you is information that is relevant to the terrorist threat, or would that really go to the FBI more than to you?

Mr. SMITH. Probably more to the FBI. But I will say that again, as you probably know, there is a protective intelligence portion of the Secret Service. We're concerned about threats, particularly those involving our techniques and that sort of thing.

So there is certainly, post 9/11, a lot more interaction, a lot more communication among the agencies, as there should be. And so quite often, we will get leads from either the intelligence community or other law enforcement agencies on the very things that you're talking about, certainly that involve the technique. We have a high interest in that.

But for the most part, it would be either the intelligence agencies or probably the FBI in terms of counter-terrorists.

Mr. ROGERS. It seems like to me overseas is Secret Service. I knew the answer to that question. I'm glad you pointed to that aggressively.

What I want to get to is: Do you work with the Justice Department and the FBI to provide the same computer forensic service to them as well? Do they have a separate agency that does what this one does?

Mr. SMITH. Again, post 9/11, there is a lot more sharing than there ever was before.

Chairman BACHUS. So FBI agents would apply to you to come here in an effort to train?

Mr. SMITH. We have not done that. This is primarily State and local law enforcement who train here.

Mr. FINCHER. Do you know where the FBI gets this kind of training?

Mr. SMITH. Within their own venue. I think they do have training, and I think they take it down into other things out there through the National Institute of Justice and so forth. I'm really not qualified to speak too far in depth on that, but I believe they do.

Mr. ROGERS. What about local law enforcement who has not been able to get in in this community—and this would be the attorneys office here, sheriff, whatever—that's not had the opportunity to get one of their personnel sent here for training? Do they have the opportunity to just send the hardware over here for analysis?

I understand that the ideal is to have the investigators working the case go through it because they know pig trails they may want to go down. But in the absence of that, can they just send hardware over here to be analyzed with some ideas about what they're looking for and then you send a report back?

Mr. HILLMAN. Yes, sir, they can. In the back of this facility is the Birmingham or the Alabama ECTFS, Electronics Training Task Force, who belong to the Secret Service that we are partners in.

Those investigators back there have the ability and the training and the wherewithal to take in those cases from different agencies.

The evidence room back there is full of cases that have been brought to us by other law enforcement agencies that don't have this kind of training or equipment, and we help them out.

Mr. ROGERS. And how much of a backlog—how many weeks and months of a backlog do you have in analyzing that hardware?

Mr. HILLMAN. We're able to turn it around pretty quickly. Before we established these in our Alabama Computer Forensics labs that you gentlemen helped us start, the turnaround time on evidence that I know is going to the FBI was somewhere around 2 years.

With those labs, with the ECTFs, we are able to turn it around generally within a matter of days, if not a week or two at most. And we prioritize items when they come in. If we have a pretty hot case, a murder case, an abduction case, a really hot financial fraud case, we put that at the top of the stack, and we work those first and we can turn it around in a matter of hours or days.

Mr. ROGERS. Do you have experienced counsel at the Federal level? I know the Department has its own intelligence besides the security officials. Of course, the FBI does.

Do you have a clearinghouse, if you get a tip or information from analyzing one of the computers that may relate to a terrorist threat, you share that with a larger group of intelligence officials?

Mr. SMITH. Yes, sir, we do. And that goes on the intelligence side of the house. We have a Director of the Secret Service who is responsible for protecting intelligence, and that goes to them. They interface and communicate quite literally daily with the other intelligence entities around the country.

Mr. ROGERS. The 9/11 Commission found that one of its biggest concerns is stove-piping, information sharing in Federal agencies. In your opinion, is that stove-piping problem gone?

Mr. SMITH. As I said a minute ago, there certainly is a lot more sharing of information than there was before and—

Mr. ROGERS. It's not a guess.

Mr. SMITH. I don't know everything that's going on. There's always that possibility. But I think from our perspective, certainly we share information. I think that the other Federal agencies, both within the Department as well as outside the Department, certainly the Justice Department and others, we have excellent relationships with.

If I could add just a follow-up about our electronic process. As I mentioned, we have 31 task forces across the United States and 2 in foreign countries now. They as well take in computers that need to be imaged that may be the results of searches or other crimes and that sort of thing. Certainly, there is a priority put on the major crimes.

But they are—we do work for most any agency that asks again whether it—it might be as financial crime or whether it involves pornography—or any other crime related to computers, which touches almost everything now.

These task forces that are around the country do that. And they do respond to the local agencies and other Federal agencies which occasionally ask for help.

So outside the perimeters here, I will be glad to have a briefing schedule for you and provide some more information about exactly the amount of work they do.

Mr. ROGERS. I appreciate that. I asked Mr. Warner this question before. I was waiting for what would hopefully be a second round of questions. I don't want to take up all your time.

Mr. Warner, I want to talk about your priorities. And what is your greatest unmet need here in your view?

Mr. WARNER. I think the greatest unmet need is the ability to open cases. And what I mean by "open", most phishing cases, for instance—phishing is the—

Mr. ROGERS. Define "phishing."

Mr. WARNER. Phishing is when a counterfeit bank Web site is created by a hacker. They make a site that looks just like the real financial institution's Web site, and they usually break into someone's Web site and add that content onto their server.

My lab has identified 180,000 counterfeit bank Web sites so far. We see 521 new counterfeit bank Web sites on a daily basis.

One of my students was doing research for his master's thesis—interviewing the heads of security for very large banks, the top 10 banks, and asked as one of his questions, what percentage of those phishing cases do you believe are investigated by law enforcement? The highest number he got was perhaps 1 percent.

These are not being treated like crimes. Someone performs a computer intrusion where they break into a Web server. They counterfeit a bank Web site. They send out spam illegally through Botnets pretending to be the bank, which they're not.

They steal the personal financial information, and then they take the money out of the victims' accounts, and no one is investigating that as a crime, because they say the bank will give you your money back.

So that's the biggest challenge for me. How do we turn that into a crime that someone is going to investigate?

Mr. ROGERS. Seeing that need, what do you need to meet that need in a more responsible fashion?

Mr. WARNER. We have the evidence. We need law enforcement people who have time cleared out of their schedule to deal with that evidence.

You spoke about the Homeland Security priority, and I firmly believe that's a very important priority. But for an example, we established a firm identity on a particular criminal whom we knew had stolen information from more than 1.4 million Americans. The field office where that crime was being worked, the agent was told he was not to work on any cases that did not involve terrorism. They didn't have anyone free to work on something as low priority as 1.4 million people having their money stolen. Even though we already knew the criminal's identity, there just wasn't enough manpower to work on it.

Mr. ROGERS. Thank you, Mr. Warner.

Chairman BACHUS. Mr. Fincher?

Mr. FINCHER. Yes, sir. Thank you, Mr. Chairman.

Back to Mr. Warner. Can you tell where most of these hackers, where they were? Where are they?

Mr. WARNER. Sure. Most of the sophisticated hacking that we see is coming from Eastern Europe. These are Russians, Estonians, Ukrainians. Primarily, Ukraine has the most talented computer programmers, the people who create computer viruses. Most of the low-tech crime comes from Nigeria. The truth is, it's just a funnel of money going overseas and no one's stopping it.

If someone steals $70 million, that's a Federal investigation, and there have been some fantastic arrests just recently on those type of cases. But who's going to help you when somebody steals $600 from your wife? No one.

Mr. FINCHER. What type of oversight or regulation do you think is needed to tighten this gap? It kills me as a Republican to talk about the government always skimping when more regulation is needed.

Mr. WARNER. One of the things is that the criminals are very aware of our current policies. For instance, one of the best ways to identify someone stealing money out of bank accounts is to do what's called an ACH wire transfer, an automated clearinghouse financial transfer.

The most common identifier that it's a criminal is if you suddenly have lots of transactions between $9,500 and $9,900. The criminals know if it's $10,000, it's a suspicious activity report.

As long as they keep below the thresholds, they feel safe. We have to start, as I already mentioned, reporting every cyber crime as a crime.

Mr. FINCHER. Mr. Hillman, the cost of people coming here and time, how much time does it take to run through the process?

Mr. HILLMAN. Actually, Congressman, I'm glad you asked that question.

When we established this facility, it was our agreement with the Secret Service to work—my guys who work with me and I are fond of saying, "The answer is money, what's the question?"

When we started putting this thing together, the greatest need in law enforcement was for money and training. We knew that the law enforcement agents who would come here would not have the money to pay. And so, we decided to take care of that.

When we vet a candidate and we select that candidate, whether it be State or local law enforcement, a prosecutor or a judge, we fly them in, we house them, we feed them, and we train them.

In a couple of cases, the network intrusion course and the true forensic course, the 5-week course, we send them home with equivalent software that we just trained them to use.

The only outlay of dollars that they have as an agency is to cover that officer's shift while he's gone.

Mr. FINCHER. What does it cost?

Mr. HILLMAN. Right now, with the annual appropriation coming from NPPD and Homeland Security through the service and out to here, it is about $4 million. And for that, you're getting roughly 400 bodies, give or take, depending on what classes we schedule and how we do that.

One other thing, Congressmen, if I may, that we haven't even touched on yet is the aspect of cell phone forensics. That is a completely different animal on how you extract that data.

Most of the things that we're seeing now are moving toward cell phones, PDAs, the iPhones, those types of things. We have to get on top of that because we're seeing that tidal wave of digital evidence coming our way, and that requires a different set of skills to get to that evidence.

That is one of the things that we have been working on with the Secret Service. We have changed our curriculum this year to add a cell phone class as well as a social networking class, which is another way the bad guys can get to you and get to your financial information and that sort of thing.

So we will definitely need—to answer your question, we definitely need help in the area of cell phone forensics as well.

Mr. FINCHER. My last question is for the Shelby County sheriff's guy.

Being from a rural county, so rural we don't even have a traffic light in my county—

Chairman BACHUS. No traffic lights.

Mr. FINCHER. No traffic lights in my county, Crockett County. We're pretty small.

Chairman BACHUS. You need to invest in infrastructure.

Mr. FINCHER. But we're not going to raise taxes.

What can we do, because we have great law enforcement but it is sophisticated and it is passing us by?

What can we do to be more productive and to get more of our guys into facilities like this?

Mr. HAMMAC. Sir, I'm going to echo Mr. Hillman and Mr. Smith's statements. This training is absolutely necessary. The need though is, I would say, volume.

Though we have had some well-qualified folks who have come through these doors and go back to their agencies not only working for their agencies but neighboring agencies, they quickly discover—the phrase around here is, "If you build it, they will come."

Their computer labs are quickly overflowing with evidence and requests. Before we realize it, we're so backlogged that we're virtually ineffective in getting the evidence turned around in a timely manner.

The answer is, we need additional resources. We need backup as the police say. We need some additional bodies who are there to help us and assist us in this fight on the front line.

And that's beneficial in the sense that many of these cases we investigate carry us across multiple jurisdictions and across State lines. Having the confidence to say we will reach out to a neighboring law enforcement agency several States away, they're going to have the capability to assist us in this investigation at the part that we are in.

Mr. FINCHER. Okay. One more question, Mr. Chairman. This is—I guess, Mr. Smith, what types of financial institutions and their customers are most at risk for cyber attacks, larger banks with more assets or smaller banks? And how at risk are community banks for cyber attacks?

Mr. SMITH. One of the things that we have seen—and again, in my prepared remarks, we talk about the Verizon studies that the Secret Service participates in.

The first few years of this, we saw the larger entities more often than not attacked, the larger banks. And a lot of times, they already—and certainly since a lot of these attacks have occurred, they have placed a lot of security measures within their systems to protect them.

So of late, the trend has been more of what you're saying, smaller banks, smaller businesses and that sort of thing. And I think the criminal is a criminal is a criminal. They're going to always take the path of least resistance.

So when you harden up one side of the house, they're going to go for the softer side. And a bank, because they have not been involved in hacks or breaches of the smaller businesses, if you will, for a period of time, now that the other side has hardened up, we're seeing more of that.

Chairman BACHUS. I want to thank—specifically, I want to compliment the Secret Service. There have been many cases where financial institutions' computers have been compromised and there's fraud going on over a matter of hours or days, and it is the Secret Service that calls and informs these banks that their systems have been compromised, and it's hard to put a dollar amount on how valuable that is.

As I said, everything from ATMs to their entire credit card operation, so you have done an extremely good job. And I think what Mr. Warner mentioned is that you are up against some of the most sophisticated criminal organizations in the world.

Some of these organizations have several hundred, is my understanding—several hundred members. And they are highly skilled, and you have had some real international successes.

On occasion, I think these people travel from time to time. And I think that local law enforcement, their training here will assist in criminals being apprehended, and it gives you more eyes in the field.

I can also say that the 900 or 1,000 people who train here is probably not an altogether accurate figure in that these people go back and train other people.

We have had the head of the whole LAPD forensic task force who was in here probably 2 years ago. When he came here, he was swapping information and techniques that he had already learned with other departments and with the staff here. And I guess you would call it almost a cross-pollination. It was exchanging information.

And, of course, his intention was to go back and train the LAPD. He was very impressed. This was a career officer who was very excited about—and he was actually a specialist already. And so that whole department—I'm sure we'll never know how many crimes they solved.

So I think there's a $4 million a year investment by the Secret Service. And just a few of these cases being just financial fraud, and then we have cases like child pornography, rape cases, child predator cases where people are killed.

It's hard to put a number on when you catch one of these people. I think we know and the legislators know and law enforcement knows that child predators repeat these crimes. They don't just kill one child. They don't just kidnap, rape, and murder one child. They're going to continue to do that until they're caught. They're going to continue to abuse children.

And financial fraud, these people are going to continue to do it until they're caught.

I had a case where a Congressman in Texas contacted me about a suspected child abuse involving sexual abuse. And we were able to get the name of someone who was within another county, an officer who had been trained here. And that person was able to assist them in that investigation.

So I don't know how many times that has happened, but I would—if any of you wish to comment—I know you're dealing with these organizations in Eastern Europe, and there's only so much that you want to share your techniques or the extent of that. But there have been some incredible successes.

They are, I guess, incredibly sophisticated—in fact, in many cases, these people are much more sophisticated than our guys. Their techniques and their operations are far more sophisticated than Al-Qaeda. And, several of them become multimillionaires. So they have the financial resources, too.

But do any of you wish to comment further?

Mr. SMITH. I would add, Mr. Chairman, in regard to what was said about the fact that these criminals can be anywhere. Certainly, a lot of them are outside the United States. And as you heard, a lot of them are in Eastern Europe. So it's through the training that the State and local agencies get here and then a portion of us trying to share some of our expertise with them, not that we're total experts. But again, we're trying. We do recognize these things.

In fact, just last month we officially opened a Secret Service office in Tallinn, Estonia, which is in the Baltic region, because again, so much of the computer crime and cases such as that originate in that area or that region.

So we try to be as proactive as we can. And again, it goes back to that cross-pollination or force multiplier methodology.

We try to take that beyond the borders of the United States. And that's why in all of the foreign offices that we have around the world, we use the same methodology that I described earlier for our investigative mission. We try to recruit—have good liaison, good cooperation with the local entities there, whether it is the local law enforcement or the State militia or whatever the law enforcement entity in that country might be.

And as I said a moment ago about our Electronic Crimes Task Forces, we extended that as well. We recently just opened two ECTFs: one in London, England; and the other one in Rome, Italy.

And quite frankly, the one in Rome, Italy, has a lot of interest in it, particularly from private sectors. The law enforcement entities are involved and interested, but also Post Paliano, which is the equivalent of the head of the postal service—is the chairman of the ECTF out there as far as quarterly meetings are concerned.

So we try to gain as much expertise as we can outside of the United States, because again, as the professor mentioned, that's quite a problem there.

Chairman BACHUS. Okay. These are very risky operations because some of these people and some of these countries care nothing about retaliating. And then there is a hatred or an envy of the United States. So it's amazing how many of these people don't think there's anything dishonest about stealing money from American citizens. It's almost regarded as a noble profession.

And it's very hard. Sometimes, the locals do not prosecute those crimes, although the Secret Service has had greater success in breaking those barriers. But I know you are basically overwhelmed.

A hundred hard drives will fill the library of Congress. Probably somewhere in America, there are 100 hard drives in the last week that have been recovered.

And one of the things about the training that the Secret Service gives local law enforcement officers and that also other local law enforcement officers here is that they learn how to, as I said earlier, extract this information. It can be on the computer. But if you don't have the expertise and if you don't have expensive software—we're talking about, what, $14,000 or $15,000 worth of software, sometimes the most advanced software. And the criminals are always one step ahead.

It's just like with counterfeiting. They have become more and more sophisticated. Now, we have a new hundred-dollar bill coming out, which will stop them for awhile. But it's a daunting task.

But I'm very grateful myself that the Secret Service has seen fit to partner with our local, State, and Federal agencies. It's a must. And I give you high marks because a lot of times Federal agencies, just like State and local agencies, focus on their jurisdiction. They are protective of that. And you have not shown any inclination to do that.

These are resources that could be diverted and that are probably diverted from some of your own operations to this operation. So, we're very thankful.

As I mentioned at the start, the testimony offered in the Casey Anthony case, that lady was very well trained and she was equal to the defense attorneys. She was probably one of the finest there was.

Judges go back and train other judges. Judge Joiner knows this. If one has the training, that judge in a circuit will try all those cases. He may try all the cases involving complex forensic matters.

He will teach his fellow jurists. He will go to courses and law enforcement training courses, and they will train other people.

And some of these departments will see what the software is here and they'll buy it and such. And I'm sure a lot of that is going on.

Mr. ROGERS. Thank you, Mr. Chairman. I want to go back to the subject matter I was talking about with Mr. Smith here earlier.

I would point out to the folks that these field hearings are congressional hearings just like we have in Washington. The primary purpose of a congressional hearing, whether it's in Washington, D.C., or here, is to weigh in on the information and that helps us develop policies. That's why you see this lady over here taking everything down.

When I was talking with Mr. Smith earlier about the number of people going through it and what the need is, there's a reason for that.

One of the problems that I found on the Committee of Homeland Security for years is it's hard—and the same thing is true for the defense of the Armed Services Committee which I serve. We try to get information out to people who know it so we can make a better policy.

The problem is, Mr. Smith has a boss who works for the Secretary of Homeland Security who works for the President who has been given a number. And that's your budget, and you salute and say yes, sir, and make it work.

I don't work for their boss. My job is to make a policy. So I'm trying to get Mr. Smith here what he needs.

If Mr. Smith tells me what he really needs, it may cost more than $4 million a year, which means his boss is going to get mad at him because his boss is going to get in trouble with the Secretary.

So having said that, I'm going to talk to Mr. Smith again.

My preacher says if you want to know what somebody's priorities are, you look at their checkbook register and their calendar. Wherever they spend their time and money is what their priorities are.

My priority is protecting the homeland. Cyber security is critically important. And that partnership between the Federal Government, State, and locals is absolutely essential.

So I look at the numbers we're talking about—we're training about 8 people per State in this technology. That seems inadequate to me.

And I understand we have budget constraints, but the Department of Homeland Security has nearly $50 billion a year to spend.

And some of it is being wasted. That doesn't mean we can't shift it over here.

So having said that, what's the number we need? Nobody is paying attention. You can tell me.

Mr. ROGERS. Be careful.

Mr. SMITH. Could I just refer to my earlier testimony? That way, I won't contradict myself.

Mr. ROGERS. You will be amazed how many generals I have come to me and state, I talked to you privately. That doesn't help me if it's not on the record.

Really, there has to be some number that you think this entity could meet that is reasonable that would give you a better reach into the problem areas that we have. And if you don't want to tell me—Randy, maybe you will be able to tell me?

Mr. SMITH. I would like to defer to Mr. Hillman on that.

Mr. HILLMAN. Congressman, I will tell you very quickly, $16 million a year would put us at capacity and start to scratch the surface on the needs that we have in law enforcement.

Mr. ROGERS. So you think you have to be at capacity?

Mr. HILLMAN. I think—no, sir. We're going to do with what we have, the best we can. But if we are at capacity, we—you talk about the force multiplier that Mr. Smith was talking about. It will get even larger and larger.

Think about this, Congressman. We're losing probably $100 billion a year if not more to financial fraud in this country every year. Think about when this committee considered—and I can't remember—I don't know what the protocol was, but they gave the TARP money and bailout to financial institutions. I don't know how many billion dollars that was, 600-plus billion dollars.

If they're losing a hundred billion dollars a year in this country, you're feeding money in this arm and they're hemorrhaging out of this arm to fraud and phishing. It doesn't take long for that $600 billion to just wash out and go overseas or somewhere else.

All we're asking for is a very small investment in law enforcement that will help prevent some of that stuff and will cover some of those dollars that are going to Estonia and Latvia and—

Mr. ROGERS. If you had $16 million, you said a little while ago that 40 percent of your applicants are being approved. Do you think that applicant pool will grow?

Mr. HILLMAN. Absolutely.

Mr. ROGERS. How much of the—you have a $4 million a year budget.

Mr. HILLMAN. Yes, sir.

Mr. ROGERS. I know that you prevent some crimes, have successful prosecution that recoups money.

Do you get a pool of ceased assets which you're able to participate in the distribution of that to help sponsor this entity?

Mr. HILLMAN. It depends on what type of crime you're working. Generally, when we get into the larger financial crimes—we join in with Ms. Vance's office, the U.S. Attorney's office. They have asset forfeiture divisions and they have asset forfeiture laws that help us draw in those assets, whatever we can put our hands on.

Mr. ROGERS. What percentage of your budget each year is pooled into assets?

Mr. HILLMAN. None.

Mr. ROGERS. So you haven't been able to generate this so far?

Mr. HILLMAN. Not that I know of.

Mr. ROGERS. How about you, Mr. Smith?

Mr. SMITH. We do receive funding from TEOAF, but again, that is for very specific new initiatives normally with a 2- or 3-year life span startups.

So our relationship, if you will, is very, very good with TEOAF and the funding that we receive for them which we put toward our investigative mission almost in total. And that goes toward major case funding and the purchase of equipment. That again is sort of a force multiplier. There's part of that money that eventually could help to buy equipment to solve a crime that somebody was trained here who ultimately uses that piece of equipment.

I know that's a very convoluted answer, but that is sort of the way that we have to operate. TEOAF, as an entity, determines how much money we get each year, but of the amount they give us, we put almost 100 percent of it toward investigations.

Mr. ROGERS. The last question I'm going to ask, I know Mr. Smith says it's not for him. Mr. Warner, I know that there have been major players in the computer world who have suggested lately that to help prevent phishing and spam, there be an Internet charge for mass mailings like that per email. That sounds like a tax to me. But if it's only for mass distribution, do you feel like it's practical or there are problems with that?

Mr. WARNER. Yes, I can answer that. The problem, though, right now, Mr. Congressman, is that criminals don't use the Internet the way you and I use it. The criminal is not registering an account and paying his bills. He's sending out millions of emails and soliciting.

The criminal is breaking into your home computer and sending the email through your home computer.

Mr. ROGERS. Then I'm against it. That's a tax on me.

Mr. WARNER. Right. The criminal's email sending—we have seen Botnets broken down by the FBI in the last year where one particular criminal could send 14 billion emails each day. He did that by having a network of over 3 million computers all around the world that were sending spam on his behalf.

Mr. ROGERS. Thank you very much, Mr. Chairman. That's all I have.

Mr. FINCHER. I just have a couple more points.

Chairman BACHUS. He wants a traffic light.

Mr. FINCHER. I'll leave it like it is, Mr. Chairman. It's very rural.

So many times, we don't appreciate what we have until we don't have it anymore. And so many times, you guys aren't appreciated enough for what you're doing. That's why it's crucial that we focus at length today—Mr. Rogers focused on the financial side, and I want to stay with that, staying ahead of the criminals because it's becoming such a liability issue that if they hit us right and hit us hard enough, it will take us down big time.

It's so important. Mr. Chairman, I go back to this. It seems like every conversation—and this is why we have been so focused, not to get political, to get our economy moving again and get people back to work and get revenue rolling again, because we can fund the things that are important.

These things are very important. Should there be requirements, you think, like Tennessee? Should it be mandatory, or maybe at the State level, that at least one person for each county comes through here? Because there are so many things slipping through the cracks that they can't see until it's too late. And we actually can see it. It has cost us how many billions of dollars? But if the money was there and we could do what we need to do here, you guys could do what you need to do, should that be something that is looked at, or is it one per State and then the States can take it or one per district? What do you think, just your opinion?

Mr. HILLMAN. Congressmen, when we look at those candidates—and I'll let Mr. Smith respond as well—you have to look at the pockets of crime and where the hot spots are. You're going to have more in Los Angeles than you will in a rural county in Nevada.

So we have to pay attention to that, and they do a very good job of looking at those areas and you kind of concentrate assets there.

On the flip side of that, in South Alabama, one rural county, there might not be another investigator who knows how to do this for five or six counties. So you want somebody there so that you don't have to drive all the way to Birmingham to find an investigator who's capable of doing it.

I don't know that you could put a requirement like that on it because it's moving all the time, and it depends on what type of crime. A whole bunch of variables go into that.

You have to—you're talking about financial crimes. Think about it. Every dope dealer is going to send text messages. You're getting capital murder cases set up with emails now. So it just really depends.

But the key thing is getting bodies out there who know what they're doing and can handle this evidence, because it's coming down on top of us very quickly, and we are way behind the eight ball in catching them.

Mr. FINCHER. Two more things, Mr. Smith: one, what is the greatest expenditure at the training center; and two, kind of go through the jurisdiction of how we deal—as Mr. Warner said a few minutes ago—with these guys all over the world and do we have problems with trying to beat that back?

Mr. SMITH. I think as far as the institution is concerned, the costs are fairly equally divided. Out of the $4 million, it's fairly equal between the travel costs, the per diem costs to the individuals while they're here as well as the equipment costs. If you look at that across-the-board, it is pretty equal.

In terms of the jurisdictional issues that I spoke about a moment ago, in the Secret Service at least, we take that force multiplier approach. We use our foreign offices to liaison and try to always have good relationships with law enforcement there. And that works for us on two levels. First, on the protective mission, because so many of our protectees travel abroad constantly now. So we need that. And that is on one level how we interact quite a lot with the host countries or countries that our protectees may visit.

But at the same time, those field offices in those foreign countries are assigned to the Office of Investigations, so they come under our office. And to the other side of the mission with the investigations, we use that same formula to try to incorporate the work that we are doing with the host country. Sometimes, we're able to actually lend some expertise to them because this is a new arena for law enforcement agencies in those countries as well. And so we try as best we can to brief them or give them some adequate training.

And as someone said earlier, some of the countries are easier to deal with than others. We have had great success in a good number of them. Particularly in some of the eastern countries, we have been successful not only in making arrests, but actually being able to extradite a few people along the way.

Mr. FINCHER. Thank you guys for your service.

Chairman BACHUS. Let me close by saying that the Secret Service investigates financial, cyber crime, and counterfeiting. Admission to this institute is somewhat restrictive, and there is a lot of demand for this center or institute. The feedback has been very complimentary. They come here and learn how to investigate other types of crimes, which are not under the charge of the Secret Service.

So the $4 million that you're spending is a small investment—I'll say if they break into my bank account, that's one thing. If they harm my grandchild, that's quite another.

So the Secret Service is rendering a valuable service outside their primary charge. And I'm very appreciative of that.

We also have had briefings on financial service. I think you were there. Some of what you're up against is pretty overwhelming. And that's also a demanding area.

I think maybe some others need to step up and find other funding sources to help fund this.

The Secret Service is the primary agency and will have jurisdiction over it, but there may be other ways to help fund it. Do you know what I mean? I'm open to any suggestions.

I do want to let the record show that I have been very nice to the Secret Service. Without objection, the hearing—

Is there anyone who wants to make a final comment? This, I think, has been a very good hearing. And the testimony—without objection, the hearing will remain open for thirty—

Judge COLE. Mr. Chairman, I apologize for interrupting. My name is Karen Cole. I'm a trial judge from Florida, and we have our entire class of trial judges here today. And I just wanted to let you know that we are grateful for what you are doing and we are particularly grateful for the Institute for what we are learning here today. There is nothing like this institute available in our jurisdictions, and we need to be able to understand the testimony when it is presented to us by law enforcement, and that's what we're learning here today. Thank you so much for the work you do.

Chairman BACHUS. Great. There are 26 judges in your class?

Judge COLE. Yes.

Chairman BACHUS. Would you—I think time will allow. I would like for you each to stand up and give your name and your jurisdiction, if that's okay, your State or your city.

Judge COLE. Jacksonville, Florida, Circuit Judge Karen Cole.

Judge LEIBER. I'm Dennis Leiber from the Circuit Court of Kent County, Grand Rapids, Michigan.

Judge HIGGINS. I'm Cheryl Higgins, Circuit Judge for Albemarle County, Virginia.

Judge STAAB. I'm Tracy Staab, Spokane Municipal Court in Washington.

Judge MCGINNIS. Mark McGinnis. I'm a trial judge in Appleton, Wisconsin, and part of the faculty here.

Chairman BACHUS. Thank you.

Judge LANDENBURG. My name is David Landenburg. I'm representing the domestic violence coordinating issue with regard to cyber crimes that pop up every day, and I'm from Tacoma, Washington.

Judge DEASON. Donald Deason. I'm a trial judge, District Court Judge from Oklahoma County, State of Oklahoma.

Judge GIACOMO. I'm William Giacomo. I'm a Justice of the United States Supreme Court, Westchester County, New York.

Judge HOORT. I'm David Hoort. I'm a circuit judge from Ionia County, Michigan, and I think we have about seven traffic lights.

Judge CUNNINGHAM. James Cunningham, Jr., from Anoka County, Minnesota, right outside Minneapolis.

Chairman BACHUS. Okay.

Judge JARRETT. Lisa Jarrett. I'm a District Court Judge, Trial Division, in San Antonio, Texas.

Judge MORRIS. I'm Judge Denise Langford Morris from the Oakland Circuit Court in Pontiac, Michigan. But more importantly, I'm a former Assistant United States Attorney. And I can't tell you how much we feel comfortable and satisfied with what we are receiving this week and more so impressed with the staff here.

The staff is impeccable from the moment that we were accepted. Thank you.

Judge KENNEDY. John Kennedy, Superior Court of New Jersey, Newark.

Judge BERGER. Wendy Berger. I'm a Circuit Court Judge in St. Johns County in St. Augustine, Florida.

Judge KRUEGER. Kurt Krueger, a Trial Court Judge in District Court, Butte, Montana.

Judge EVANS. My name is Michael Evans. I'm a Superior Court Judge in Kelso, Washington.

Judge NEWMAN. Clifton Newman. I'm a Circuit Court Judge from Columbia, South Carolina.

Judge MOORE. I'm Daniel Moore. I'm a Circuit Court Judge and Major Felony Court Judge in Clark County, Indiana, near Louisville, Kentucky.

Judge MILLER. I'm Rich Miller. I'm a District Judge from Madill, Oklahoma. I was told by a lot of the OU football fans that they were treated more graciously than they had ever been treated when they played Alabama in 2003. I have to agree. It's so nice and has been such a wonderful experience to be able to come here today.

Judge VERSTEEG. I'm Pat VerSteeg. I'm an Associate District Court Judge from western Oklahoma. In my home county, we have no traffic lights either.

Judge BRNOVICH. Susan Brnovich, Superior Court in Maricopa County, Arizona.

Judge SNYDER. Irvin Snyder. I'm a New Jersey State Superior Court Judge. I serve in Camden County, which is just outside of Philadelphia. And we have a traffic light on every corner.

Judge CRAWFORD. I'm Charlie Crawford, Circuit Court Judge for Viera, Florida. I'm proud to come home. I'm a graduate of Cumberland School of Law.

Judge MEYER. I'm Sam Meyer. I'm a District Court Judge of Thurston County, which is in Olympia, Washington.

Chairman BACHUS. That was very inspiring. And Mr. Smith and Mr. Hillman, I think that was very—they were very complimentary of the center. And I would ask the judges, who are always very influential people in their towns and cities, to talk to their local Members of Congress and tell them about the value that you received here.

And we appreciate the job you have done. We appreciate your sacrifice for coming here and staying and applying yourself to what is a complex set of issues, and it's a complex field of the law. And you obviously—it speaks well of you that you are participating and would more better serve your constituents. So I think it's a compliment to you. And we are just overjoyed to have you.

Now, Tony, that has to make you feel good as Mayor of Hoover.

Mayor PETELOS. Absolutely, Mr. Chairman.

Chairman BACHUS. With that, I want to recognize Wayne—is it Pacine—who is the interagency project manager for the Board of Governors of the Federal Reserve System.

Thank you for being here. And Greg Garcia, who is the FSSCC chairman of the cyber committee. Is he here?

Okay. All right. Thank you very much, and this hearing is adjourned.

[Whereupon, the hearing was adjourned.]

APPENDIX

June 29, 2011

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..."

[1] Identity-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.

<u>The challenge for law enforcement</u>

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.

Testimony of Randall I. Hillman

Executive Director, Alabama District Attorneys Association

Esteemed members of the Financial Services Banking Committee, Governor Bentley, honorable members of the Alabama Legislature, other guests and my respected colleagues in law enforcement,

In the last 25 years criminal justice community has witnessed two watershed events with respect to criminal law; first is the advent of DNA evidence. The second, and the reason we are here today, is the creation and proliferation of digital evidence and cyber crime.

In my current position as the Executive Director of the Alabama District Attorneys Association, it is my daily job to analyze and attempt to meet the needs of law enforcement and prosecutors. Without question, the need for digital evidence training is the one of our most pressing. The meteoric escalation of digital evidence can be compared to a tidal wave looming over the criminal justice community. This type evidence is present in the majority of all criminal cases now, whether it is identity theft, phishing, child pornography or murder or any other crime. The question is, do we as law enforcement agents and prosecutors have the means to gather that evidence. The answer in most cases is a resounding "no".

Ladies and Gentlemen, you know better than most anyone else that we cannot stick our proverbial head in the sand. We must endeavor to be ahead of the curve. We must be ahead of the criminals who would pray on our family's financial security. This effort starts at home. When I was a child, the bank was a brick building in the center of town that you walked into and deposited a check or withdrew money. Today, we can access our "virtual bank" literally anywhere. This convenience, although desirable, makes us extremely vulnerable to criminals. I would submit to you that not one individual in this room has not had their personal data, or financial holdings compromised in some way due to a surreptitious intrusion by a cyber criminal. We are not immune and neither are our children. They are by definition, prime targets for identity thieves because they have identifiers that are considered "pristine" because they generally will not discover that their identity has been compromised for several years. This gives the criminal a very long time to use their identity fraudulently. We are breeding a crop of young adults that will undoubtedly exist entirely on technology based banking and commerce. Today our kids and young adults have credit cards, PayPal accounts, play station credit accounts, wii accounts and Apple APP accounts. Each of these areas are fertile grounds for a cyber criminal. And once one of these accounts is compromised who will we call? More often than not it will be your local police department or your local prosecutor who will be asked to investigate and prosecute the bad guys.

Additionally, at the opening of this facility in 2007, Chairman Bacchus stated that terrorists such as Osama Bin Laden were using technology and the internet to fund and to manage their worldwide terrorist networks – most often by identity theft, bank fraud and phishing. Recently his comments were proven true after the capture and killing of Bin Laden. Bin Laden had in his possession hundreds of computer disks and digital devices containing priceless evidence that will be used to understand terrorist networks and ultimately help eliminate them. Similarly, domestic and international terrorists and common criminals fund their criminal enterprises through the use of cybercrime and digital devices. They do this by compromising banking systems through network intrusions and stolen identities. This not only cripples our banking industry and financial institutions but devastates our citizens. Some would say this is strictly a federal matter, but I wholeheartedly disagree. Over 95% of all criminal cases are originated and tried in state courts. Those officers on the street, the first responders are absolutely critical to building an identity theft or network intrusion case and will, in the end, provide the key evidence that will convict criminals and provide restitution for victims.

Members of the Committee, it is imperative that all law enforcement agents and prosecutors be given ability to protect your constituents. It is both shocking and tragic that law enforcement is ill equipped and trained to respond to a digital crime scene. I submit to you that the only way we can change this is by greatly expanding training for law enforcement and prosecutors and by helping provide them with the equipment they need to do their jobs properly. Unless and until we do these things, thieves, scammers, pedophiles and other criminals will continue to go unpunished because they know that we simply do not have the ability to catch them.

Chairman Bachus, Senator Richard Shelby, Alabama's District Attorneys and my staff at the ADAA set out to address this problem head on. We had experienced the lack of quality computer forensics training first hand. Our trials in attempting to find trained law enforcement agents and prosecutors to staff our own Alabama Computer Forensics Labs were the catalyst. Because no one entity made it their mission to train law enforcement, prosecutors and trial judges in digital evidence, we were left in a very difficult position of staffing these labs. This facility, the National Computer Forensics Institute, is a direct result of this need and the unprecedented cooperation of all levels of government, from the highest federal agencies to the smallest local governments. This facility focuses on all computer related crimes with an emphasis on financial crimes, and more importantly, is taught by true investigators who have been and are now in the field each day. They understand and teach the curriculum from a law enforcement perspective, not that of an academician or a layman. I witness each and every day the inherent value of quality digital evidence training and education here and I know that the graduates from this facility have both solved thousands criminal cases and have prevented many others from being committed.

In closing I would like to thank you for being here. Members of the Committee and other distinguished guests, your presence is both a sign and a promise that you are committed to a unified front against cyber criminals. Furthermore, I respectfully challenge you to join me and my colleagues in law enforcement to ensure that training facilities like NCFI that train authorities to investigate, prosecute and even prevent financial cyber crimes and other crimes remain as one of our top priorities.

Randall I. Hillman

Executive Director

Alabama District Attorneys Association

Statement of Mr. A.T. Smith
Assistant Director
Office of Investigations
U.S. Secret Service

Before the Committee on Financial Services
U.S. House of Representatives:
"Hacked Off: Helping Law Enforcement Protect Private Financial Information"

June 29, 2011

Good afternoon Chairman Bachus, Ranking Member Frank, and other distinguished Members of the Committee. Thank you for holding this hearing at the National Computer Forensics Institute (NCFI) and for giving the U.S. Secret Service (Secret Service) the opportunity to discuss our role in protecting cyberspace, particularly as it relates to the safeguarding of our nation's critical financial infrastructure. We are proud of the training program that has been established at this facility and look forward to working with Congress to ensure its continued success.

The Secret Service's dual mission of investigations and protection has evolved over the course of the last century, not because we seek new responsibilities but because the criminal methods used by our adversaries are constantly evolving. Based on our history as an investigative bureau of the Department of Treasury, the Secret Service has jurisdiction to investigate all forms of financial crimes including identity theft, false identification, mortgage fraud, and counterfeit checks. Given that the majority of these crimes today are committed via electronic means, the Secret Service has become very active in the investigation and prevention of cybercrime. As a result of these investigations, and with the development of specialized training programs to equip our agents with the skills needed to gather forensic evidence to successfully prosecute these crimes, the Secret Service's work is critical to the protection of both physical assets and computer networks upon which our economy and our communities rely.

National Computer Forensics Institute (NCFI)

The investigative mission of the Secret Service cannot succeed without the cooperation of local and state law enforcement, the private sector, and academia. Law enforcement and judiciary officials from all over the United States come here to the NCFI for vital digital forensics training necessary to protect our nation's financial infrastructure, commerce, and well being of our citizens. The NCFI is a testament to the essential cooperation needed to fight the ever evolving cyber threats faced in our increasingly interconnected global community.

The NCFI, which is a result of a partnership between the DHS National Protection and Programs Directorate (NPPD), the Secret Service, the State of Alabama, the City of Hoover, Shelby County, the Alabama District Attorney's Association, and the Alabama Securities Commission, was established to provide computer forensic training and tools to state and local law enforcement officers, prosecutors, and judges to conduct computer forensics examinations. Investigators are trained to respond to network intrusion incidents and conduct electronic crimes investigations. This training also has the benefit of providing state and local law enforcement with the skills and tools to combat a myriad of crimes in their community.

Since the establishment of the NCFI in 2008, DHS-NPPD has transferred $4 million annually to the Secret Service to train state and local law enforcement officials, prosecutors, and judges on the importance of computer forensics to criminal investigations. Responding to the growth of cyber crimes and the level of sophistication these criminals employ requires training, resources and greater collaboration among law enforcement and its public and private sector partners. Thus far, 644 state and local law enforcement officials, 216 prosecutors, and 72 judges representing over 300 agencies from all 50 states and two U.S. territories have received training from the Secret Service through the NCFI. After initial participation in the program, 80 NCFI students have returned to take one or more advanced courses at the Institute over the last three years.

Collaboration Among State, Local, Federal, and International Law Enforcement

While strong collaboration between federal agencies and our international counterparts is critical, there is an increasing awareness that stronger partnerships with state and local law enforcement, prosecutors, and judges are essential to protecting our nation's critical infrastructure. Just as there is recognition that our local first responders are on the front lines of natural disasters and other homeland security challenges, so too must we recognize that many of today's cyber crimes are first investigated by local law enforcement.

In 1995, the Secret Service formed its first Electronic Crimes Task Force (ECTF) in New York City. The concept brought together not only members of federal, state and local law enforcement, but also members of academia and the private sector. Cooperation was needed at all levels to fight this new type of electronic crime that was constantly evolving, often faster than the laws and regulations in place to protect financial infrastructure. Perhaps one of the most important results of this task force was the close partnerships our agents developed with state and local law enforcement, prosecutors, and judges.

The ECTF concept has been replicated in other Secret Service field offices throughout the nation and in two locations internationally. Local law enforcement and judiciary are not only fighting cyber criminals locally, they are assisting in fighting threats that are emanating from outside the United States which directly affect our citizens and commerce. The NCFI therefore provides crucial training to support our mission and enhances the capacity of local law enforcement to combat a myriad of crimes. Advances in computer technology and greater access to personally identifiable information (PII) via the Internet have created a virtual marketplace for transnational cyber criminals to share stolen information and criminal methodologies. As a result, the Secret Service has observed a marked increase in the quality, quantity and complexity of cyber crimes targeting private industry and critical infrastructure. These crimes include network intrusions, hacking attacks, malicious software, stolen credit, debit and ATM card data and account takeovers leading to significant data breaches affecting every sector of the world economy.

The increasing level of collaboration among cyber-criminals raises both the complexity of investigating these cases and the level of potential harm to companies and individuals. For example, illicit Internet carding portals allow criminals to traffic stolen information in bulk quantities globally. These portals, or "carding websites," operate like online bazaars where criminals converge to trade personal financial data and cyber-tools of the trade. The websites vary in size, from a few dozen members to some of the more popular sites boasting membership of approximately 80,000 users. Within these portals, there are separate forums moderated by notorious members of the carding community. Members meet online and discuss specific topics of interest. Criminal purveyors buy, sell and trade malicious software, spamming services, credit, debit and ATM card data, personal identification data, bank account information, brokerage account information, hacking services, counterfeit identity documents and other forms of contraband.

Over the years, the Secret Service has infiltrated many of the "carding websites." One such infiltration allowed the Secret Service to initiate and conduct a three-year investigation that led to the indictment of 11 perpetrators involved in hacking nine major U.S. retailers and the theft and sale of more than 40 million credit and debit card numbers. The investigation revealed that defendants from the United States, Estonia, China and Belarus successfully obtained credit and debit card numbers by hacking into the wireless computer networks of major retailers — including TJX Companies, BJ's Wholesale Club, OfficeMax, Boston Market, Barnes & Noble, Sports Authority and Dave & Buster's. Once inside the networks, they installed "sniffer" programs that would capture card numbers, as well as password and account information, as they moved through the retailers' credit and debit processing networks. After the data was collected, the conspirators concealed the information in encrypted computer servers that they controlled in the United States and Eastern Europe. The credit and debit card numbers were then sold through online transactions to other criminals in the United States and Eastern Europe. The stolen numbers were "cashed out" by encoding card numbers on the magnetic strips of blank cards. The defendants then used these cards to withdraw tens of thousands of dollars at a time from ATMs. The defendants were able to conceal and launder their fraudulent proceeds by using anonymous Internet-based electronic currencies within the United States and abroad, and by channeling funds through bank accounts in Eastern Europe.

While cyber-criminals operate in a world without borders, the law enforcement community does not. The increasingly multi-national, multi-jurisdictional nature of cyber crime cases has increased the time and resources needed for successful investigation and adjudication. The partnerships developed through ECTFs as well as the support provided by our Cyber Intelligence Section (CIS) and the training provided to our special agents via Electronic Crimes Special Agent Program (ECSAP) were all instrumental to the Secret Service's successful investigation into the network intrusion of Heartland Payment Systems (HPS). An August 2009 indictment alleged that a transnational organized criminal group used various network intrusion techniques to breach security, navigate the credit card processing environment, and plant a "sniffer," a data collection device, to capture payment transaction data.

The HPS investigation – the largest and most complex data breach investigation ever prosecuted in the United States – revealed that data from more than 130 million credit card accounts were at risk of being compromised and exfiltrated to a command and control server operated by an international group directly related to other ongoing Secret Service investigations. During the course of the investigation, the Secret Service uncovered that this international group committed other intrusions into multiple corporate networks to steal credit and debit card data. The Secret Service relied on various investigative methods, including subpoenas and search warrants, to identify three main suspects. Mutual Legal Assistance Treaty (MLAT) requests submitted by prosecutors were also sent via the Office of International Affairs (OIA) of the Criminal Division to foreign countries requesting evidence. As a result of the investigation, the three suspects in the case were indicted for various computer-related crimes. The lead defendant in the indictment pled guilty and was sentenced to twenty years in federal prison. This investigation is ongoing with over 100 additional victim companies identified. The Secret Service is working with our law enforcement partners both domestically and overseas to apprehend the two defendants who are still at large.

Collaboration within the federal, state and local law enforcement community enhances information sharing, promotes efficiency in investigations, and facilitates efforts to de-conflict in cases of concurrent jurisdiction. For example, the Secret Service has collaborated extensively with the Department of Justice's Computer Crimes and Intellectual Property Section (CCIPS), which "prevents, investigates, and prosecutes computer crimes by working with other government agencies, the private sector, academic institutions, and foreign counterparts."[1] The Secret Service's ECTFs are a natural complement to CCIPS, resulting in a strong partnership over the years. In the last decade, nearly every major cyber investigation conducted by the Secret Service has benefited from CCIPS contributions.

The recent arrest of an individual charged with being one of the world's most notorious traffickers of stolen financial information, serves as an excellent example of successful cooperation between the Secret Service and its law enforcement partners around the

[1] U.S. Department of Justice. (n.d.). *Computer Crime & Intellectual Property Section: About CCIPS.* Retrieved from http://www.justice.gov/criminal/cybercrime/ccips.html

world. The suspect is alleged to have created the first fully automated online store for selling stolen credit card data. Working with our international law enforcement partners, the suspect was identified and apprehended as he was boarding an international flight to Russia. Both the CCIPS and the OIA of the Department of Justice played critical roles in this apprehension. This type of cooperation is crucial if law enforcement is to be successful in disrupting and dismantling criminal organizations involved in cyber crime.

More broadly, the Secret Service maintains an excellent relationship with the Federal Bureau of Investigation (FBI). The Secret Service has a permanent presence at the National Cyber Investigative Joint Task Force, which serves as the coordination and integration center for the identification, mitigation, and neutralization of both criminal and national security threats against the United States. In the last several years, the Secret Service has partnered with the FBI on various high-profile cyber investigations. For example, in May 2010, a joint operation involving the Secret Service, FBI and the Security Service of Ukraine (SBU), yielded the seizure of approximately 143 computer systems – one of the largest international seizures of digital media gathered by U.S. law enforcement – consisting of approximately 85 terabytes of data

Within the Department of Homeland Security (DHS), the Secret Service works closely with NPPD's United States Computer Emergency Readiness Team (US-CERT), which provides response support and defense against cyber intrusions or incidents for the Federal Civil Executive Branch (.gov) domain, as well as information sharing and collaboration with state and local government, industry and international partners. As the Secret Service identifies malware, suspicious IPs and other information through its criminal investigations, it shares information with US-CERT. The Secret Service looks forward to building on its full-time presence at US-CERT, and broadening this and other partnerships within the Department.

As a part of these efforts, and to ensure that information is shared in a timely and effective manner, the Secret Service has personnel detailed to the following DHS and non-DHS entities:

- NPPD's Office of the Under Secretary;
- NPPD's National Cyber Security Division (US-CERT);
- NPPD's Office of Infrastructure Protection;
- National Cybersecurity and Communications Integration Center (NCCIC)
- DHS's Science and Technology Directorate (S&T);
- Federal Bureau of Investigation's National Cyber Investigative Joint Task Force (NCIJTF);
- Each FBI Joint Terrorism Task Force (JTTF), including the National JTTF;
- Department of the Treasury – Terrorist Finance and Financial Crimes Section;
- Department of the Treasury – Financial Crimes Enforcement Network (FinCEN);
- Central Intelligence Agency;
- Department of Justice, International Organized Crime and Intelligence Operations Center;
- Drug Enforcement Administration's Special Operations Division;

- EUROPOL; and
- INTERPOL.

The Secret Service is committed to ensuring that all its information-sharing activities comply with applicable laws, regulations, and policies, including those that pertain to privacy and civil liberties.

Private Sector Partnerships

The Secret Service believes that building trusted partnerships among all levels of law enforcement, the private sector and academia is the right model for addressing the challenges of securing cyberspace. It is through such wide-ranging and established partnerships that the Secret Service is able to help expand the collective understanding of cyber crime and continue to augment our prevention, advanced detection, and prosecution efforts. A recent example of our collaboration with the business community involved a joint 2010 Data Breach Investigations Report with Verizon, which analyzed more than 900 breaches, involving more than 900 million compromised records. The widely disseminated report offers recommendations to assist the private sector in securing their networks from both internal and external threats. The recently released 2011 Data Breach Investigations Report (http://www.secretservice.gov/Verizon_Data_Breach_2011.pdf) examined 800 new data compromise incidents since the 2010 report. The 2011 study includes input from The Netherlands' National High Tech Crime Unit.

Network intrusions and cyber crime can be devastating to companies of any size. Theft of data and customer information often has more dire consequences on a small- or medium-sized company that may not have the resources or expertise necessary to properly protect their networks and data. The NCFI adds to our ability to support the private sector during times of crisis by providing the tools and training that local and state law enforcement need to protect businesses, large and small, across the United States.

Successful Cyber Investigations as a Result of NCFI Training

The NCFI initiative has led to numerous successful cyber investigations. For example, a forensic examiner from the Alabama Computer Forensic Laboratories attended the Network Intrusion Responder (NITRO) course offered at the NCFI. After completing the three-week course, he began to work an investigation involving individuals filing fraudulent federal and state tax returns online with a total loss in the hundreds of thousands of dollars. Using skills learned in the NITRO course, he constructed a decoy network to capture all unauthorized network traffic at the consenting owner's Internet connection as well as assisting in securing the owner's real network. The examiner recovered key forensic evidence proving the suspect accessed the decoy network and conducted criminal activity at the online tax website.

Another example of a successful cyber investigation conducted by an NCFI graduate is in July of 2009, the Arapahoe County Sheriff's Office received a complaint from a mortgage lender in the city of Centennial, Colorado. The mortgage lender found more than 40 applications for payday loans, totaling approximately $200,000, originating from the same IP address. A graduate of the NCFI began to focus on the network intrusion leads in the case, and was able to determine that the logins used were stolen from the account belonging to the owner's wife. The IP address came back to a residence outside of Las Vegas owned by a former employee of the mortgage lender who had knowledge of the company systems to enable him to commit these crimes. Based on the electronic evidence recovered in the investigation and the suspect's home computer, he subsequently confessed to the scheme.

In addition to traditional cyber-related financial cases, NCFI graduates have been able to use the skills learned in the classroom to recover key evidence in traditional criminal investigations. In 2009, an 11 year-old boy was taken from his home near Saginaw, MI. Within hours local law enforcement developed a suspect, a former caregiver / babysitter, and a search warrant was executed on the suspect's residence resulting in the seizure of five computers. A graduate of the NCFI was contacted to conduct a forensic review of the electronic media and, within minutes, the officer recovered evidence from the suspect's computer placing him in an area near Sandusky, OH. Local police were contacted to search a nearby amusement park and found the suspect's car in the parking lot. Less than two hours after the information was located on the computer the child was found unharmed and the suspect was apprehended.

Conclusion

As more information is stored online, target-rich environments are created for sophisticated cyber criminals. With proper network security, businesses can provide a first line of defense by safeguarding the information they collect. Such efforts can significantly limit the opportunities for these criminals. Furthermore, prompt reporting of major data breaches involving sensitive personally identifiable information to the proper authorities will help facilitate a thorough investigation.

The Secret Service is committed to safeguarding the nation's financial payment systems by investigating and dismantling criminal groups involved in cyber crime. Responding to the growth of these types of crimes and the level of sophistication these criminals employ requires significant training, resources and greater collaboration among law enforcement and its public and private sector partners. Accordingly, the Secret Service dedicates significant resources to improving investigative techniques, providing training for law enforcement partners and raising public awareness. We will continue to be innovative in our investigative approach to cyber crime and cyber security and we are pleased that the Committee recognizes the magnitude of these issues and the evolving nature of these crimes.

Thank you again for this opportunity to testify on behalf of the Secret Service and share some of the many positive impacts of the National Computer Forensics Institute. I will be pleased to answer any questions at this time.

Protecting the Public through Government, Academic, and Industrial Partnerships

Testimony of Gary Warner
Director of Research in Computer Forensics
The University of Alabama at Birmingham

Congressman Bachus and members of the committee, I would like to begin by thanking you for the opportunity to testify this afternoon, and for the vision of the committee that has lead them to hold this important hearing today. We are especially fortunate to be in this facility, the National Computer Forensics Institute, an organization that has trained hundreds of state and local law enforcement officers to be able to respond to today's complex crimes that often involve digital evidence found on the computers, phones, and servers that we rely on to protect our identities, our finances, and our intellectual property.

At UAB, the University of Alabama at Birmingham, we are also engaged in that protection effort. Our contributions are in three main areas.

> Through our teaching, we prepare the next generation of cybercrime investigators, computer forensics examiners, and computer security professionals, who will both design more secure systems and investigate those who breach them.
>
> Through our research, we develop tools, techniques, training, and intelligence to assist the current investigators, examiners, officers, and analysts, by combining the knowledge of computer scientists and criminologists in ways that enable a leveling of the playing field when facing ever more sophisticated criminals.
>
> Through our outreach, we educate and inform the public about protecting themselves from online threats through lectures and conference presentations, social media and blog posts, and traditional media outlets such as newspapers, magazines, and television.

Today's hearing is entitled "Helping Law Enforcement Protect Private Financial Information." My testimony today will outline some of the issues that currently allow financial information to be regularly stolen, and then discuss some of the ways Law Enforcement is working with Academia and Industry to move beyond these problems.

Before I start, allow me to provide a few brief definitions.

Phishing – Phishing is the crime of gathering personal information through subterfuge by imitating a website or official communication from a trusted organization, such as a financial institution. The complexity of the information gathered ranges from a simple userid and password to allow access to an online account, to full information including credit card or ATM numbers, PINs, Social Security Numbers, Drivers License information, or answers to common security questions such as Mother's Maiden Name or High School Mascot.

Malware – Malware is software which will perform an unauthorized or harmful action on a computer. Non-technical people would usually call this a computer virus, which is one of several types of malware.

Botnet – A botnet is a collection of computers which are controlled by malware to cause them to do the bidding of a criminal. Each individual computer on a botnet has been compromised by criminal malware and is referred to individually as a "bot." The criminal usually controls his botnet through a "Command & Control" or "C&C" server. The criminal controlling a botnet is often referred to as a "botherder." Criminals use botnets for many types of activities, including sending spam emails, stealing personal information or documents, launching crippling attacks on other computers, or allowing the criminal to anonymize their true location by "proxying" their network traffic through the bot computer.

Keylogger – A keylogger is a particular type of malware which steals information typed by the computer user and provides a means for the information to be retrieved by the criminal. Keyloggers are often used to steal personal financial information without the knowledge of a victim simply by observing the victim interacting with his or her online financial accounts.

Protecting Private Financial Information from Cyber Threats

Critical Infrastructure Protection, Phishing, and Law Enforcement

My very first research into phishing was a natural outgrowth of my interest in Critical Infrastructure Protection. In 1997, President Clinton convened a Commission on Critical Infrastructure Protection which resulted in goals that were stated in Presidential Decision Directive 63 (PDD-63) including that by the year 2000 we would have significantly increased the security of government computer systems, and that by 2003 we would be prepared to protect the critical infrastructures of our country from all threats, both cyber and physical. PDD-63 established the National Infrastructure Protection Center and sector specific Information Sharing and Analysis Centers. Beginning September 6, 2001, the energy company for which I then worked hosted the first InfraGard meeting in the Birmingham area, and Special Agent Mike Mauldin explained the concept of Critical Infrastructure Protection to an audience of sixty local companies including all of the largest banks in the state.

In 2002, Ron Dick, then the Director of the National Infrastructure Protection Center was speaking with me at the National InfraGard Congress. I mentioned that sometimes people asked me why I spent so much of my time on Critical Infrastructure Protection issues. His response probably changed my career path that day. He reached into his pocket and took out a White House lapel pin, pinned it on my jacket, and told me, "You tell them because the President of the United States asked you to, that's why!"

I took that very seriously, and that is exactly what the President asked us all to do with PDD-63, which established the need for Public-Privater Partnerships:

> "Since the targets of attacks on our critical infrastructure would likely include both facilities in the economy and those in the government, the elimination of our potential vulnerability requires a closely coordinated effort of both the government and the private sector. To succeed, this partnership must be genuine, mutual and cooperative." – PDD-63, May 22, 1988

Three years later when the banks in my InfraGard chapter began to have problems with phishing they turned to law enforcement for help, but they also turned to the computer security professionals who were members of the local InfraGard chapter. No one in law enforcement had seen this type of cyber attack before, and we had to figure out questions like "What is the crime?" and "Who is the victim?" There was a great deal of confusion. The then-current version of Title 18 Section 1030 stated that it was a federal crime to hack the computers of a financial institution, but wasn't clear about hacking a website belonging to an individual and using that website to pretend to be the bank! Today we have great laws making it a crime to compromise any computer attached to the Internet, but those laws are not being enforced in this area.

Just as Bill Clinton said in PDD-63, and George Bush re-iterated in Homeland Security Presidential Directive 7 (HSPD-7) and in the National Plan to Secure Cyberspace, and President Obama has said while appointing Howard Schmidt to serve as Cyber Security Advisor, we need to work together in order to stop these crimes. Birmingham, like 24 other cities, is fortunate to have both an InfraGard chapter and a US Secret Service Electronic Crimes Task Force. I have hosted both organizations in my lab, have donated students from my lab as interns to work in the computer forensics lab here in the National Computer Forensics Institute in support of law enforcement, and have stood in this building to present about phishing to a group of more than forty Alabama-based banks who had been brought together by the Electronic Crimes Task Force. We need the increased cooperation, because the problem is worse than ever.

Issue One: The increase in cybercrime far outpaces the increase in law enforcement focus on cyber

When I began investigating phishing crimes in December 2004, along with my InfraGard banking associates, we learned of the Anti-Phishing Working Group, a non-profit organization that had taken on the challenge of coordinating information about phishing. That first month, the Anti-Phishing Working Group reported there had been 1707 unique phishing sites documented that month, or a rate of about 55 new phishing websites per day.

In the first quarter of 2011, UAB saw 47,452 unique phishing sites for 300 different online brands and businesses. That is 521 cases of computer intrusion per day, with more than 50% of those computers located in the United States. Numbers for the second quarter were nearly the same with 46,134 nphishing sites attacking 303 online brands.

Almost all of those phishing sites are on hacked webservers. We're now documenting and gathering evidence from more than 15,000 phishing servers every month. More than half of those servers are located in the United States.

A report from the APWG last month[1] indicated that not only are there are dramatically more phishing websites, they are staying online longer than ever before.

What other category of crime has increased by 900% over the past seven years?

Part of the increase in online crime is a response to the increase in the online economy itself. In 2000 there were only 360 million internet users and the entire e-commerce environment was only $5 billion. Only 18% of the American public had ever used online banking! In the first quarter of 2011 by comparison, online retail sales reached $46 Billion, or 4.4% of all retail sales. 2010 online sales accounted for $164 Billion of our economy last year[2], a 3200% increase in the past decade. While the Internet only contributes 3.8% to the GDP in the United States, it accounts for 21% of the GDP growth in the past five years, making a greater contribution to GDP than Agriculture, Utilities, or Mining.[3]

The other change impacting online crime is the international demographic of the Internet itself. In 2000, the majority of those 360 million internet users were in the United States and subject to our laws. As of the first quarter of 2011 we now have 2 billion Internet users, but only 13% of them are in North America.[3] 87% of Internet users are in other countries, but the largest concentration of wealth accessible from the Internet remains in the United States.

Part of this growth has been that many more criminals are choosing to explore the area of phishing as a way to make money. Another part of the increase, however, is that criminals have embraced technology to a deeper level than law enforcement. For more advanced criminals, creating a new phishing site is literally only one mouse click. With a single click of the mouse, their programs scan the internet for a website with a well-known vulnerability, compromise the website, upload the counterfeit bank website to the compromised server, and begin to send spam messages warning consumers of a problem with their bank account and inviting them to visit the phishing site to resolve the problem.

We need a corresponding growth in our ability to use technology to investigate these cyber crimes, and that is one focus of our lab. Law enforcement officers and agents from the FBI, Secret Service, the Alabama Department of Public Safety, the IRS, four Attorney General's offices, and many state, local, and international law enforcement officers can now log in to the UAB PhishIntel system to gain evidence of phishing crimes with a click of the mouse as well.

Despite these growing numbers of phishing sites, the banks tell us that they are even more concerned about malware than they are about phishing. Several senior banking security officials tell us that they estimate losses due to malware are three times as high as those due to phishing.

[1] "Global Phishing Survey: Trends and Domain Name Use in 2H2010", Aaron, G., Rasmussen, R. April 27, 2011. http://www.antiphishing.org/reports/APWG_GlobalPhishingSurvey_2H2010.pdf

[2] U.S. Census, "Quarterly E-Commerce Retail Sales Report", May 16, 2011, http://www.census.gov/retail/mrts/www/data/pdf/ec_current.pdf

[3] "The Internet Matters", McKinsey and Company, May 2011, http://www.eg8forum.com/fr/documents/actualities/McKinsey_and_Company-internet_matters.pdf

This weekend, the UAB Spam Data Mine documented a spam email message that we received more than 60,000 times. The email message simply said "It's Bob's New Car!" and had a link to a website, claiming to show you a picture of the new car. The name was randomly generated, so that your email may have said Bob, Chris, David, or any one of thousands of names. If you clicked the link, the website you visited asked you to download and execute a Photo Archive called "archive.exe". Many tens of thousands of people visited the website, although most were too well-educated to actually run the program. Unfortunately, just by visiting the website more than twenty separate cyber attacks were launched against their computers. If they didn't have the current patches for Windows, Internet Explorer, Opera, Java, Adobe Reader, or Adobe Flash Player, the criminals would be successful in secretly causing a copy of the Zeus trojan to be downloaded and executed on their computers.

Zeus is a "keylogger" trojan. At that point, every userid and password the infected computer user types, for everything, is sent to the criminal. Email passwords, banking passwords, Facebook passwords, online shopping passwords, work systems, any password they type, along with the accompanying information about what system or website was being accessed when the password is typed, is sent to the criminal.

Because this is the Zeus trojan, the criminal can then come back to the infected computer, at any time they choose, and take remote control of the system. They can use YOUR computer with YOUR userid and YOUR password to log in to your bank account, and transfer your money anywhere they please. They can also retrieve any document on your computer and install any additional software they please. They can send emails that come from you. They can order things with your credit card. They can change your passwords! They can send instant messages (with links to viruses!) from your Instant Message or Chat program AS YOU to all of your friends.

Home users may lose hundreds of dollars each, but business banking accounts suffering losses due to a Zeus infections can approach $1 million per incident. Just this month two lawsuits on this situation have been resolved with contradictory opinions about who is responsible when a business customer loses big money to a trojan.

On June 8, 2011 the headline was "Bank dodges legal bullet over Zeus trojan lawsuit".[4] Patco Construction of Sanford, Maine was infected with the Zeus trojan. The trojan took their banking password and, logging in to their account at Ocean Bank from the construction company's computer, caused $588,000 to be transferred out of the account. The bank said it was the consumer's fault for not protecting their computer from viruses. The consumer said it was the bank's fault for not having adequate authentication measures. In this case, the bank won.

Just one week later, however, on June 15, 2011, the resolution in a second lawsuit went the other way. In that case the headline was "Court Favors EMI in Fraud Suit: Judge Says Comerica Bank Should Have Detected Wire Fraud."[5] In this case, Experi-Metal, Inc. had more than $1.9 Million in wire transfers

[4] "Bank dodges legal bullet over Zeus trojan lawsuit", Info Security News, June 8, 2011.
http://www.infosecurity-us.com/view/18512/bank-dodges-legal-bullet-over-zeus-trojan-lawsuit/

[5] "Court Favors EMI in Fraud Suit", Bank Info Security, Kitten, Tracy. June 16, 2011.
http://www.bankinfosecurity.asia/articles.php?art_id=3750

leave their bank account. The finding in this situation said the bank, not the customer, was responsible despite the fact that the customer's computer was the source of the compromise.

In the example about the "New Car" malware website advertised by spam, one could argue that users should know not to click on a suspicious link in email, but the risk is nearly universal at this point. In 2009, the New York Times was tricked into running a fake Vonage advertisement on their website that infected visitors with a virus. Any consumer that visited the New York Times website during the time that the malicious advertisement was in place would have a high chance of having a Zeus trojan successfully installed on their computer. The same types of malicious advertisements have been seen on many other websites, including Yahoo! and Google webpages.

Issue Two: Lack of computer science, high performance computing, or data mining to process evidence

At UAB, some of the Computer Science specialty areas where we do research include high performance computing, knowledge discovery & data mining, natural language processing, and distributed computing. Having these resources available to draw from, the UAB Computer Forensics Research Laboratory has taken a unique approach to analyzing evidence related to cyber crimes. Our laboratory has been fortunate to receive both a COPS Technology Grant from the Office of Community Oriented Policing Services, and a Byrne Grant from the Bureau of Justice Assistance, which have been combined with contributions from the Microsoft Digital Crimes Unit and the Alabama 10th Judicial Circuit District Attorney's office to create a unique environment for gathering, analyzing, and reporting on the evidence of cyber crimes.

In our lab we have three primary focus areas: spam, phishing, and malware. In each of these areas we are building Computer Science-based solutions to deal with very large quantities of evidence.

One of the challenges faced by law enforcement in the area of personal financial information being stolen is to be able to recognize the scope of the crime. Last summer we reported on a case worked by the Federal Trade Commission that I described in my blog as "Stealing $10 Million, 20 cents at a time."[6] In this case, the FTC had identified that the criminals had made 1.3 million fraudulent charges against consumer credit accounts ranging in value from 20 cents to $10. Imagine that you were a law enforcement official in a local police department receiving the phone call that someone has stolen $6 from the victim's bank account? 90% of the victims never filed any form of a complaint.

There are parallels to this type of case in spam, phishing, and malware cases.

The UAB Spam Data Mine and the UAB PhishIntel system are two systems that allow us to assist law enforcement with understanding the scope of a particular criminal activity. Because we receive a

[6] Cybercrime & Doing Time blog, "Stealing $10 Million, 20 cents at a time", Warner, Gary, July 3, 2010, http://garwarner.blogspot.com/2010/07/stealing-10-million-20-cents-at-time.html

million new spam messages per day and have more than 500 million spam email messages archived in the UAB Spam Data Mine, we can answer questions of scale and connection with regards to digital evidence.

Last month a law enforcement agency in the state of Alabama received a complaint from a citizen who had received an email purporting to be from a senior government official. Working in the UAB Spam Data Mine, we were able to determine that this was a unique email message, and provide suggestions to the investigator on how to proceed based on the very unique nature of the message. In this case, the account which sent the email was only one day old, and it was possible to prove that only a small handful of messages had been sent from the account, and that there was only one victim, indicating that the attack may have been personally motivated.

In what sounds at first to be a nearly identical complaint, another law enforcement agency received a complaint from a citizen about an email that claimed to be from the FBI. The email message indicated that the citizen had visited more than forty illegal websites and claimed that because of this, they were required to fill out the questionnaire that had been attached to the email. The attachment was actually malware that would add the computer to a botnet if the attachment was opened, leading to a potential loss of all personal information to the cyber criminal. Unlike the Alabama complaint, where the evidence would show that a single sending computer had targeted a very particular victim, in this case the UAB Spam Data Mine had received 54,720 identical email messages on the same day as the victim. We were able to identify that these messages were sent by a botnet with at least 26,928 different computers, and that it was likely tens of millions of others had received the same email. By being able to provide detailed reporting on the other activities of the botnet over time, as well as the location of each machine which had sent spam to UAB, our lab was able to help distinguish that this was a major cyber crime ring with potentially thousands of victims, as opposed to a lone wolf actor performing a revenge attack against one individual.

Issue Three: Lack of Criminal Complaints Leads to Lack of Intelligence

A problem we are facing in the fight against financial crimes is that the criminal complaint has almost disappeared. Even when a police report is filed, it is often "so the bank will give you your money back. Case closed."

The understandable hesitation of law enforcement to "work a case" in these areas has lead to an unfortunate form of apathy by the consumer as well as the financial institutions. Large banks lose millions of dollars each year to phishing and malware, but they reimburse the cost to customers and structure the losses into the cost of doing business. Consumers have been trained that if they experience financial losses they should contact their financial institution rather than the police. If they have had their money returned by their financial institution, there is little incentive to share that information with law enforcement.

This also makes it less likely they will ever report their victimization in a way that allows intelligence-driven policing Internet crimes to occur. Without a mechanism to gather basic complaint data into a data mine, it becomes very difficult to understand the scope and nature of the crimes we are facing.

The FTC collects consumer complaints from a large number of sources, including the Internet Crime and Complaint Center (ic3.gov), the Better Business Bureau, the US Postal Inspection Service, and many state Attorney General's Offices. But there is still an enormous amount of unreported crime. The most recent FTC Consumer Sentinel Report[7] indicates 1.3 million complaints were received from consumers, however the best estimates indicate that there are now more than 11 million identity theft victims per year in the United States. One of the challenges is how to make sure these additional victims can have the crimes against them documented. If even the minor cases are documented properly, data mining of the complaint data can lead to significant cases being brought by linking the smaller cases together.

This is the basis for a new partnership called "Operation: Swordphish" which brings together UAB, the Alabama District Attorney's Association, and the Alabama Department of Public Safety. One of the key components of the project is to work with our law enforcement partners on Public Service Announcements and an awareness campaign on how to report financial cyber crimes effectively. UAB will provide support to our law enforcement partners by hosting a web server for people to report cybercrime victimization. These reports will be enhanced by comparing key pieces of information from the received complaints with information available in the UAB Spam Data Mine, UAB PhishIntel system and malware data mine to determine whether the case has links to prominent cybercrime outbreaks or to other Alabama-based crimes. In many cases, UAB will be aware of a cluster of related phishing websites, but may be lacking a victim.

Our Operation Swordphish partners agreed that when a case had an Alabama nexus, UAB would perform searches in our various databases to qualify or "triage" the case, and make an investigative lead to law enforcement.

[7] Consumer Sentinel Network Data Book for January – December 2010. Federal Trade Commission, March 2011. http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2010.pdf

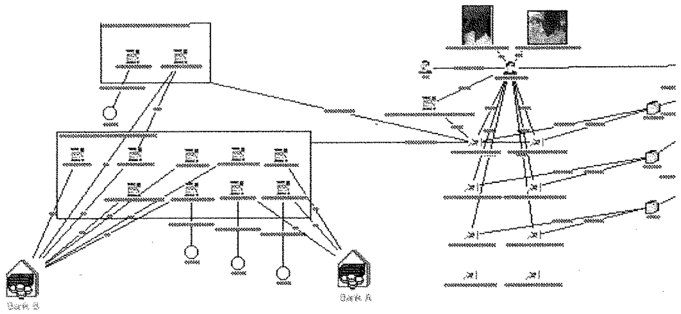


Figure 1 - An Example Operation Swordphish Case

In our first experiment in Operation Swordphish, we had identified three phishing sites for an Alabama-based bank, (Bank A) that PhishIntel showed were related by two common email addresses belonging to the criminal.

The searches revealed a small number of victims for the Alabama bank, but revealed six previously unknown phishing sites and a large number of victims for a bank in another state that we were unaware was related until the searches were performed. Several additional criminal email addresses were also revealed in the emails, including accounts that confirmed a Facebook page for the criminal.

In a second case, evidence from the UAB PhishIntel system was able to link together phishing crimes against seven financial institutions to a single criminal, based on a common email address. The criminal had hacked into three servers in order to create fake websites targeting an Alabama-based brand. UAB PhishIntel was able to provide conclusive evidence that all thirty-two phishing sites were related to one criminal. It is likely that with thirty-two known phishing sites this criminal has stolen personal financial information, and possibly funds, from hundreds of victims.

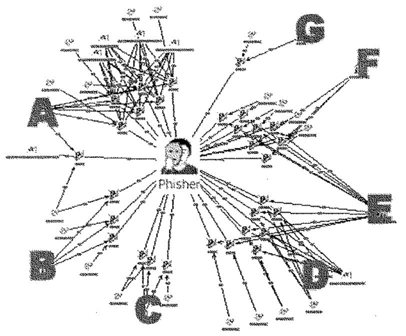


Figure 2 – In this example UAB PhishIntel links financial crimes by criminal's email

Issue Four: The international and trans-jurisdictional nature of the Internet

There are several jurisdictional issues that are faced when dealing with cyber crimes against one's personal information. One of these is that "small crimes" are normally the jurisdiction of local law enforcement while "major crimes" are more appropriate for Federal law enforcements. It is also usual that local crimes are the purview of local law enforcement while international crimes are the purview of federal law enforcement.

But what is a "local" crime on the Internet? A spammer in Nigeria sends an email to Alabama, inviting someone to visit a hacked Polish website that imitates a bank in New York. If they are successful in tricking the victim, a criminal in Romania may buy the credentials from the Nigerian and transfer the money to an account in California, where a local person removes the money and sends 50% of it via Western Union to Romania. How much money was stolen? Perhaps $500 from that victim.

It is increasingly difficult to gain law enforcement cooperation for the investigation of an international cyber crime. Some members of the committee have personal experience in this area, as servers at the House of Representatives have been compromised by website defacers from overseas. These defacements occurred in exactly the same manner in which websites are transformed into phishing sites. International gangs of hackers operate with complete impunity, boasting about their crimes and providing links to their email address, blog pages, and chat rooms in the messages they leave behind.

Website owners hosting their small business and personal websites in the United States, have had their servers hacked for use by phishing criminals more than 40,000 times so far in 2011. At the present time, I am unaware of a single situation where the hacker was arrested. Because of the experience of the crime "going overseas" many law enforcement officers are hesitant to take these cases, and local law enforcement officers question whether it is even appropriate for them to be involved in a case that is potentially international.

It is often the case that while portions of the crime may go overseas, parties to the conspiracy are located in the United States. Many financial cyber criminals have found it is easier to work with US-based accomplices to remove money from bank accounts. The most common method of doing so is to recruit a "money mule" to receive the stolen funds into an established local bank account.

Money mules often begin as disposable employees who believe they have been selected for a "work at home" job. These jobs are often advertised by spam email messages promising amazing earning potential for hard workers with little or no educational requirements or experience. A popular version at the present time is a "Mystery Shopper" position. In this position the new employee is told that they will test the customer service and friendliness of various businesses, such as check cashing businesses, bank tellers, and international money transfer services. The mystery shopper may be asked to open a new bank account and evaluate the friendliness of the bank personnel, or receive a deposit into their personal account and then evaluate the customer service of the employee at Western Union as they send the money to Eastern Europe. Some criminal organizations use several thousand money mules per year in various schemes of this sort. The advertisements promise earnings up to $300 for each assignment.

While Money Mules of the type above are likely not chargeable, many large rings of money mules continue to operate domestically with the full knowledge of their participants. Without investigating the phishing crime, the opportunity to identify this critical US-based part of the criminal enterprise is lost.

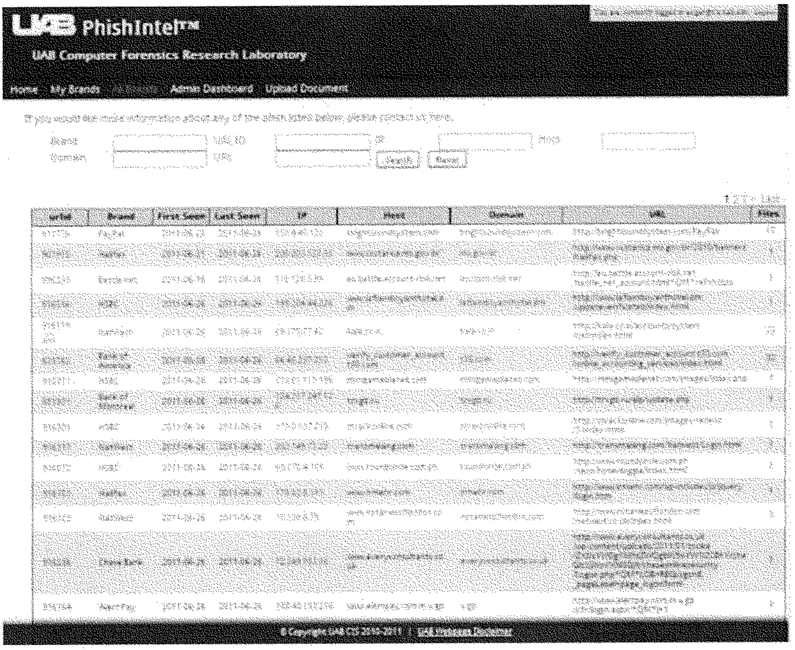
Issue Five: A Need for more trained cyber crime professionals

Others presenting testimony today will share with the committee some of the outstanding work of the US Secret Service and the National Computer Forensics Institute. We are also making a contribution at UAB by training students who will graduate from UAB with two to four years experience working in the UAB Computer Forensics Research Lab in addition to course work specifically designed to meet the needs of law enforcement cyber crime investigators.

This year UAB launched a new Masters Degree in "Computer Forensics and Security Management" which is a partnership between the Computer & Information Sciences Department, the Justice Science Department, and the School of Business.

Our outreach also involves training for current law enforcement. Specifically in the area of Phishing, we developed curriculum called "The Seven Steps of a Phishing Investigation" and presented it last October at the Digital Crimes Consortium in Montreal to over one hundred law enforcement professionals.

We continue to seek opportunities to provide more US-based law enforcement with access to our UAB PhishIntel tool, and to provide training for them in our phishing investigation methodology. PhishIntel is currently used by more than 200 users, including 70 law enforcement officers from 35 agencies.



urlid	Brand	First Seen	Last Seen	IP	Host	Domain	URL	Files
[illegible]	PayPal	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	Bank of America	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	Chase Bank	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

© Copyright UAB CIS 2010-2011 | UAB Webpages Disclaimer

Figure 3 - An example screenshot from the UAB PhishIntel portal