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