Testimony of
Tiffany O. Jones
iSIGHT Partners, Inc.

Before the
Senate Homeland Security and Governmental Affairs Committee

Regarding
"Data Breach on the Rise: Protecting Personal Information from Harm"

April 2, 2014

Chairman Carper, Ranking Member Coburn, and distinguished Members of the Committee, thank you for the opportunity to present to you today.

My name is Tiffany Jones, and I represent iSIGHT Partners, a leading cyber threat intelligence firm. Over the last seven years, we have built a team of 200+ experts dedicated to studying cyber threats in many nations across the globe and enabling organizations to protect themselves against these threats.

There are a variety of threat domains that make up the cyber threat landscape today. Each of these threat domains is motivated differently. For example, Cyber Espionage, targeted intrusion operations aimed at corporate and government entities to collect information for the purpose of a strategic advantage, can be politically motivated (stealing secrets) or economically motivated (stealing intellectual property). Cyber Hacktivism focuses on the intentions and capabilities of politically- or ideologically-motivated actors, who express their beliefs or attempt to project power through malicious or destructive online activity. Cyber Crime focuses on cyber threats from primarily financially-motivated actors.

The intelligence we research, analyze and disseminate, coupled with the scope, scale, and duration of the recent retailer attacks, leads us to one very clear conclusion: We need to stop thinking about cyber crime like the movie *Catch Me If You Can*, one clever young man assuming identities and passing bad checks.

Instead, we need to understand that cyber crime is more like the movie *Goodfellas*, an organized community of bad people, intent on crime, economically motivated, increasingly sophisticated, and operating without much fear of law enforcement.

Cyber crime is a global industry with a division of labor, evolved supply and demand, as well as a defined value chain. This chart gives you an overview of what that value chain looks like:

Step 1 – Malware: Cyber crime starts with malware. Think of this like an App Store for hackers. Thousands of developers craft hacking tools and toolkits with various features,

functions, and capabilities and sell them on a broad array of electronic markets. Prices can range from a few to several thousand dollars.

Just like an App Store, only a fraction of malware goes on to be popular depending upon the features, targeted vulnerability, usability, and other characteristics. At any point in time, there are probably a few thousand notable pieces of malware on the market with 10 new entrants that warrant analysis in a given month.

At higher price points – subscriptions of $5,000 to $15,000 per month – there is also private access to malware developers. These are the more sophisticated designers.

Step 2 – Infrastructure: Cyber criminals must obfuscate their operations. This means buying storage, computing, and network services from dedicated infrastructure operators – sort of a Criminal Cloud Computing. This is a large and varied segment of the market, everything from securing $50 domain names to $1,000 per server per month hosting arrangements. Some of these organizations can scale to multi-million dollar operations serving 1000+ criminal clients.

Step 3 – Cyber Crime Operators: Like entrepreneurs, operators assemble temporary teams, acquire tools, secure infrastructure, and execute against a plan. The better the plan, the bigger the payout. Like entrepreneurs, the very best exploit a market need, quickly monetize the value, and move on to the next opportunity. One recent operation netted as much as $3.8 million for the operator and their team in just a few short months.

Step 4 – Brokerages/Intermediaries: To monetize stolen assets in cyber crime – typically this is some form of personal data like credit card, health insurance, or social security numbers – the operators take their bulk data to brokers. Think of these players – again numbering in the thousands – as wholesalers.

The brokerages pay bulk prices to the operators for the stolen data, and then parcel it up into sizes that a larger number of smaller criminals can use. At the retail level, this looks like an underworld eBay, with prices set by the type, newness, quality, and completeness of the stolen data. More reliable sellers get higher prices.

In early December, we saw complete U.S. credit cards at $100 per card. With the dramatic increase in supply due to several recent retailer breaches, the price dropped to $50. Much of that card data is now dated and U.S. cards sell at closer to $16 per card.

Step 5 – Card Buyers & Mules: The transition from the criminal economy to the traditional economy presents the biggest bottleneck for cyber crime. Using stolen information involves risks and transaction costs, so most cyber criminals leave much of the small change on the table while focusing their efforts on big, quick hits. Card buyers and mules bear most of the risk.

The typical card buyer or a mule for receiving stolen property or bank payments is just a small-time, and occasionally unwitting, criminal – the intern of the cyber crime industry. They

get relatively small payments, if any, for relatively small crimes. They are typically involved in the illegal activity for a short time, and often have no connection with the larger criminal enterprise. Like a pickpocket who just takes the cash from your wallet – their gain is small, but your loss in time, effort, and personal value can be significant.

So, as you can see, the scope of the cyber criminal market is daunting – and the money made pales in comparison to economic value destroyed as a result. At any time, there are tens if not hundreds of thousands of independent actors. They are global. They are unregulated. They are better equipped, better trained, and more experienced than many of their law enforcement counterparts. And they are growing bolder.

You will see attacks like the 2013 retailer breaches again, and with greater frequency. Business and government has started to understand the scope of this problem, and are increasingly shifting to intelligence-led cyber security to improve prevention, speed response, and solve the cyber security risk equation. There is progress. There needs to be more of it. Thanks to government entities like Department of Homeland Security, USSS, and their awareness efforts, the severity and scope of the problem is becoming increasingly evident.

As you consider policy, here are some things to consider:

Don't:

- Seek to be technically prescriptive. Tools and tactics evolve too rapidly, so the policy responses need to be flexible. While EMV, or chip and pin, increases security on credit cards, it is not the panacea to solve all data breach problems. Additional measures, like encryption of data at rest as well as data in transit will also go a long way to protecting what the bad guys are really after: sensitive data.
- View this just as a technology problem. Cyber security, like traditional crime prevention and disaster preparedness, needs to be treated within the context of business and government management as a risk management issue.
- Equate the quantity of arrests in cyber crime with the quality of arrests – focused prosecution higher in the value chain makes a bigger impact

Do:

- Increase global collaboration. Most of these people are not inside of our borders. Without foreign law enforcement and community engagement, there will be no progress
- Focus the efforts on cyber risk management – the recent NIST framework is a good push in the right direction. Building threat more holistically into the risk framework is needed. If you do not understand your threat profile and the threats coming after you, you cannot solve for risk within your organization.
- Direct continuing NIST efforts to specifically evolve risk models that define a true ROI aligned to business/mission requirements

Thanks again for the opportunity to speak with you today. I look forward to answering any questions you may have.