Director Sullivan's Keynote Speech for the MasterCard 2011 Americas Global Risk Management Conference

April 25, 2011

Thank you, Wendy Murdock, for the kind introduction. It is my pleasure to be here today to discuss the very serious problem of cybercrime, especially as it relates to protecting the integrity of our financial payment systems. I want to thank MasterCard for the invitation to speak at this year's Global Risk Management Conference

There is no doubt that our economic vitality and national security depend on the security of cyberspace. In just the past twenty years, we have witnessed an enormous shift in the use of computers in almost every aspect of our lives – from how we educate our children, to how we communicate, to how we conduct business. I know all of you can appreciate this shift given your business, but it is worth considering some of the activities we now take for granted: many people in this room probably used the internet to book their travel for this conference, to register and pay for the conference fees, and to print off their boarding passes for their flight.

Cybercrime threatens to restrict our abilities to communicate in this modern age, to travel, to power our homes and to run the economy.

This threat requires ever evolving strategies to combat it and a strong partnership between law enforcement and industry.

Today, I would like to cover three key areas – the first is the emerging trends and tactics that we are seeing related to cybercrime. The second area will highlight what the Secret Service is doing to combat cybercrime. The third, and most important, area will highlight how your participation in industry is critical to this effort.

But before I get into the details of those three areas, it's worth mentioning why the Secret Service is involved in this effort. While we are best known for protecting The President, we also protect the financial infrastructure of this country. In fact, that was our original mandate when we were created almost 150 years ago.

As payment systems have evolved from cash, to checks to electronic systems, so too has the investigative mission of the Secret Service. Our Special Agents are highly involved in electronic and cybercrime investigations.

As a component of the Department of Homeland Security, we work to support the Department's mission to safeguard and secure cyberspace.

But to understand how to secure cyberspace, we must first understand the threats we face, which brings me to my first theme, trends and tactics in cybercrime. From experience, and I am sure all of you can relate, wherever money is found, criminals will also be found looking for vulnerabilities in the systems that protect it.

Therefore, it is no surprise that criminals are constantly looking to exploit weaknesses in cyberspace to steal from others. We find ourselves with a financial system that relies on cyberspace to ease commerce, but can also present opportunities for criminals.

While many cybercriminals look to steal money and information, there are some who also seek to destroy, disrupt and threaten the delivery of critical services. These individuals are relentless in their pursuits – they work day and night to use our dependence on cyberspace against us.

Whenever a new security feature is put in place, you can be assured that they are looking for a way around it. They do this from all around the world.

The Secret Service has observed a marked increase in the quality, quantity and complexity of cybercrimes targeting private industry and critical infrastructures. These crimes include network intrusions, hacking attacks, malicious software, and account takeovers leading to significant data breaches affecting every sector of the world economy.

The increasing level of collaboration among cybercriminals raises both the complexity of investigating these cases and the level of potential harm to companies and individuals. 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. When these online cyber fraud portals first came into existence, they boasted membership of a few hundred criminals;

today, some of these cybercrime forums boast memberships of tens of thousands of 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.

Some of these sites are supported by "bullet proof hosters", who provide web hosting services that allow their customer's considerable leniency in the types of materials their customers may upload and distribute. Here are some of the criminal activities we are seeing in our investigations:

In an operation that began in 2005 here in San Diego, which we named "Operation Carder Kaos", suspects were trafficking in millions of stolen credit cards. Many of these suspects were located in Eastern Europe and Asia.

Two of the many suspects in this case were an individual known as Delpiero, living in Bangkok, Thailand and another known as Maksik, a Ukrainian national vacationing in Turkey. Delpiero would purchase the stolen credit card data from Maksik and then would encode and emboss the numbers on high quality counterfeit credit cards obtained in China.

So, to recap, we had a Ukrainian suspect in Turkey selling information to another suspect in Thailand who purchased his raw materials in China.

As you can see, the crimes are truly international in nature and require very close coordination and partnership with the law enforcement entities in all countries involved. Both of these individuals have been arrested and Delpiero will soon be extradited here to San Diego.

Another case that highlights the complex transnational nature of today's investigations of cybercrime is that of Lucian Dragos Osanu. In this case, the Secret Service was originally contacted by the Spanish National Police in mid-2008 requesting assistance in an international credit card fraud investigation.

Spanish authorities had uncovered an organized group that was alleged to be using captured financial account information to produce fraudulent access devices. Osanu was a member of this group and had been traveling to the United States to procure credit card encoders and readers for use in this enterprise.

Based on the evidence collected during the course of the investigation, the Spanish National Police arrested and charged 30 individuals with fraudulent use of credit cards, falsifying public documents, false indication of currency, illegal solicitation and fraud.

As this investigation progressed in Spain, the Romanian Police Service for Combating Organized Crime was working with our Bucharest Resident Office on an international cyber crime investigation that also involved Osanu. The Romanian authorities were facing an organized group that was using fraudulent emails to direct victims to illicit internet pages that collected their personal information.

The group then exploited the compromised accounts using white plastic cards and making internet purchases. Osanu was providing information to this group. Ultimately, our Romanian partners arrested and charged 16 Romanian citizens with phishing and access device fraud.

In March of last year, suspect Osanu was located and arrested in Virginia on federal charges of bank fraud and conspiracy.

In another case, a suspect known as Dron was found in Canada selling high-quality skimmers over the internet. These devices were then used by other criminals to steal the information off of legitimate cards to either counterfeit or sell via the carding sites.

As a result of the joint investigative effort between the Secret Service and Canadian law enforcement, Dron has now been charged by Canadian Officials for his crimes.

In some cases, we have uncovered cybercriminals who not only sell stolen credit card data, but also run the underground websites where it is sold. For example in a case here in California, Max Ray Butler, known as Iceman, was hacking into systems to steal credit card information which he subsequently sold on his own website.

At the time of his arrest, Iceman had stolen the information from more than 1.6 million credit cards. I am happy to say that the Iceman is now on ice, serving a 13 year prison sentence for his crimes.

And then there are the bullet proof hosting cases like McColo Corporation. This Delaware Corporation was owned by a Russian national and provided web hosting services for various domestic and foreign entities. It was discovered that McColo's servers housed botnet controllers used to manage tens of thousands of compromised computers.

These servers were also used for network intrusions into online banking systems and large scale retail data breaches.

McColo advertised its services on Russian language forums associated with Cybercrime and even had customer testimonials touting its quality of service. The seizure of the entire McColo network has provided a vast amount of information for use in investigative leads.

What do these cases show us and why do they matter? The short answer is that they are complicated and they impact the lives of millions of people. They also are attacking the core of your business.

The cases are complicated not only because they are international in nature, but also because they involve a complex network of actors that range from the person selling skimmers, to the person skimming cards at restaurants, to the person selling that information on the internet, to the person acquiring numbers and using them, to the people supporting the websites via forums and web servers.

Breaking up these criminal networks requires a highly coordinated law enforcement strategy with a focus on constant innovation in our tactics to meet emerging threats. This leads me to my second theme, which is what the Secret Service is doing to help fight cybercrime.

The first thing we are doing is actively targeting the individuals who take part in these criminal activities, regardless of where they are physically located. As the previous examples highlight, we are willing to undertake complex cases that require a large investment of time to pursue criminals anywhere in the world.

While the international aspect of cybercrime still presents a range of challenges, we have established relationships through our 23 foreign field offices so that we are able to work jointly with foreign law enforcement to bring significant targets to justice. As a result, we have been able to issue international arrest notices that our international partners use to detain suspects while they are traveling abroad. These suspects are then extradited to the United States to answer for their crimes.

Through greater understanding of how the criminal world operates here and overseas, the Secret Service has also developed strategies that have a greater impact in terms of disrupting and dismantling underground networks.

Along with our domestic and international partners, we use this knowledge of criminal networks to adapt our response to the challenges posed by financial crimes in the 21st century. We are developing the technical expertise to track down and successfully prosecute cybercriminals who pride themselves on their knowledge and technical prowess.

Law enforcement has, in many cases, learned the tricks and techniques that cybercriminals use to hide their identities and their crimes and developed countermeasures that allow the perpetrators to be found and prosecuted.

For example, at the Secret Service, we have established the Electronic Crimes Special Agent Program or ECSAP. Agents assigned to this program receive highly specialized training based on the lessons learned from our investigations – making them highly knowledgeable in the current tactics of cybercriminals.

These agents use these skills as computer investigative specialists who are qualified to conduct examinations of all forms of electronic evidence.

The training we provide, however, extends past our own agents to others in the public sector. To further address cybercrime, we continue to train state and local law enforcement through our National Computer Forensics Institute initiative.

The initiative is the result of a partnership between the Secret Service, the Department of Homeland Security, the State of Alabama, and the Alabama District Attorney's Association.

The goal of this facility is to provide a national standard of training for a variety of electronic and cybercrimes investigations.

At all levels, law enforcement is also having some success in getting the legal system to recognize the seriousness of losses stemming from online financial crime.

This fact is reflected in the lengths of some of the prison sentences we have seen – a good example of this increase is the disposition of the recent TJX and Heartland cases. In March of last year, Albert Gonzalez received two concurrent 20 year sentences for his role in these network intrusions – the longest sentence ever imposed in the United States for a hacking crime.

There is little doubt that sentences of 20 years in prison will serve as a much greater deterrent than did the sentences typically seen in such cases a decade ago.

Part of this comes from law enforcement and industry's abilities to build better cases against online suspects.

Quite possibly one of the most important things we are doing to combat cybercrime is working with those of you in the private sector. Our agents have been working with many of you to address the cybercrime problem through identifying risk mitigation strategies via our Electronic Crimes Task Forces, which are partnerships between all levels of law enforcement, the private sector and academia.

We currently operate 31 of these ECTFs, including two overseas in Rome and London. By joining our task forces, all of our partners benefit from the resources, information, expertise and advanced research provided by our international network of members while focusing on issues with significant regional impact.

Also leveraging the expertise of the private sector, for the second year, the Secret Service has collaborated with Verizon on the 2011 Verizon Data Breach Investigations Report.

If you have not had a chance to review the report, I highly recommend that you pick up a copy because there is a lot of interesting information in it. A couple of statistics that I would like to mention are that 92% of the cases reviewed involved attacks that were not highly difficult, suggesting that the cybercriminals are looking for the path of least resistance in their activities. Equally interesting is that 96% of the breaches were avoidable through simple or intermediate controls.

Those controls, or mitigation efforts, included such simple tasks as ensuring that essential controls are met, auditing user accounts and monitoring privileged activity, and examining ATM's and other payment card input devices for tampering.

Our ongoing partnerships with those of you in industry leads me to my final major theme, which is what all of us can continue to do to help in this effort. With a problem this big and this complicated, there is room for all of us to do more. This problem threatens our critical infrastructure, the security of the economy and the security of your business.

I realize security is often viewed as a cost center in business, but in the case of cybercrime, proactive mitigation strategies also help to support your company's revenues. It will take the efforts of all of us to combat cybercrime.

As with this conference, all of us need to continue to educate ourselves and heighten our awareness to the issues that are out there and the threats that exist. You know that those threats will not go away – the best thing to do is find ways to mitigate them.

Applying best practices in cybersecurity is important to businesses of all sizes and protects the information of the company and the customer. As you know, implementing such safeguards are especially important for smaller organizations; in that Verizon report I mentioned, 73% of the cases reviewed involved companies with less than a thousand people.

While many of the mitigation strategies highlighted in the report were categorized as low cost, and low difficulty to implement, I know some actions could require financial resources and that many decisions ultimately come down to how it impacts the bottom line.

It's important to remember, however, that your decision not to implement safe guards also impact the bottom line – because, according to the Ponemon Institute's recent report, the average data breach now costs over seven million dollars.

Another action you can take is to consider participating in our ECTF initiative if you are not already doing so.

Those of you in this industry have a tremendous amount of expertise in areas that are crucial to impeding the activities of cybercriminals. You may be seeing trends and tactics that would be of use to those of us in law enforcement and would help us successfully disrupt these criminal enterprises.

Please do not keep that information to yourself, especially if you find that you have been the victim of an attack.

If you have been the victim of an attack, I know that you have concerns about not only the immediate impact of the breach, but also the fallout. We know that when it comes to cybersecurity issues, many companies would prefer to handle the issue internally so as not to damage their reputation and potentially their financial stability.

I want you to know that we can help and that we do everything we can to maintain the highest levels of confidentiality allowed under law related to the investigation.

If you do face this type of problem, please reach out to your local Secret Service field office for assistance.

Partnerships, in their truest form, involve information sharing, open communication and perhaps most critically – mutual trust. What we do together to secure our nation and to protect our neighbors and our communities will have a profound impact on future generations.

In closing, we have talked about the current trends and tactics, the efforts of all of us in law enforcement to combat the threat of cybercrime, and what you are doing to help.

Where does that leave us? As I said at the beginning of my remarks, electronic commerce will not go away just because cybercriminals will continue to look to identify and exploit vulnerabilities in our systems. We need to be prepared for their efforts and continue to innovate our own techniques to uncover and stop them.

I look forward to being a partner with each of you as we work together in our mutual pursuit of stopping cybercrime.

I thank you for your time today and hope you enjoy the rest of the conference.