**STATEMENT FOR THE RECORD OF**
**JOE BERNIK, CHIEF TECHNICAL STRATEGIST – FINANCIAL SECTOR, MCAFEE, LLC.**
**BEFORE THE U.S. HOUSE OF REPRESENTATIVES COMMITTEE ON FINANCIAL SERVICES, SUBCOMMITTEE ON TERRORISM AND ILLICIT FINANCE**
**ON "MONETIZATION OF STOLEN FINANCIAL AND OTHER DATA"**
**March 15, 2018, 2:00 PM | RAYBURN HOUSE OFFICE BUILDING ROOM 2128**

Good morning, Chairman Pearce, Ranking Member Perlmutter, and distinguished members of the subcommittee. Thank you for the opportunity to testify today. I am Joe Bernik, McAfee's Chief Technical Strategist for the Financial Sector. I have two decades of experience creating and implementing cyber security management programs at global financial Institutions. While serving as CISO and head of information risk and security at ABN AMRO, Fifth Third Bank and BNY Mellon, I led teams dedicated to protecting customer data, complying with data-related laws and regulations and managing incident response programs. Since May 2016, I have developed cybersecurity practices, products and standards for McAfee. I work with the broader banking industry to align McAfee's products and roadmaps to the ever-evolving threat landscape faced by the financial services industry.

I am pleased to address the subcommittee on this important matter. My testimony will address the cybersecurity challenges financial institutions face, the threats posed by state and non-state actors, what happens to stolen data and how it is used, and general recommendations that can enhance the cybersecurity capabilities of financial institutions.

## MCAFEE'S COMMITMENT TO CYBERSECURITY

McAfee is one of the world's largest cybersecurity companies, creating business and consumer solutions that help secure our digital lives. McAfee prides itself on building solutions that work with other industry peers, and we help businesses orchestrate cyber environments that are truly integrated, where protection, detection and correction of threats happen simultaneously and collaboratively. By protecting consumers across all their devices, we secure their digital lifestyle at home and while on the go. By working with other security players, we are leading the effort to unite against state-sponsored actors, cybercriminals, hacktivists and other disruptors for the benefit of all. McAfee is focused on accelerating ubiquitous protection against security risks for people, businesses and governments worldwide.

Before beginning my comments, I want to express how extremely pleased McAfee is to see the focus on improving the cyber threat landscape for financial institutions. These institutions comprise one of the most critical of all critical infrastructures. Along with governments, energy, water and telecommunications, the financial services sector is vital to the daily functioning of our economy and our overall security. Thank you for investigating ways to better protect this vital segment of our digital economy.

## THE THREAT LANDSCAPE

According to a global report the Center for Strategic and International Studies (CSIS) and McAfee recently produced on Economic Impact of Cybercrime-No Slowing Down, banks are the favorite target of skilled cybercriminals – a fact that CSIS finds has been true for a decade. Yet it is also true that financial institutions, especially in the United States, invest more in cybersecurity – in both technology and information sharing efforts – than most other sectors. Finance was also the nation's first vertical to set up an ISAC (information sharing and analysis center), and it is generally seen as one of, if not *the*, leading sector in cybersecurity preparedness. There is no doubt, however, that financial institutions are still a prime target for cybercrime, for obvious reasons.

CSIS finds that North Korea and Russia are the top two nation states perpetrating financial cybercrime. Cyberattacks provide a lucrative way to supplement the North Korean government's access to foreign currency, and Russia provides a sanctuary for cybercriminals, housing some of the world's most talented cyber felons, whose attention focuses on the financial sector.

The attacks are not always directly against the largest banks, however. In fact, targeting the "seams" between well-defended networks is becoming increasingly common. The North Korean attack against the SWIFT network is a good example of exploiting weak points in the global financial network to make off with huge sums. In that situation, the North Korean Reconnaissance General Bureau (RGB) was aware of the difficulty of executing a large-scale heist from a single major western bank. Therefore, they targeted smaller, less sophisticated banks in developing countries like Bangladesh, Vietnam and Ecuador. Once they had compromised these banks' systems, they used the banks' credentials to send SWIFT fund transfer requests to larger banks in other countries. As the requests at first appeared legitimate, tens of millions of dollars were transferred fraudulently.

This practice of not targeting the largest financial institutions directly has proven to be quite effective in other situations as well. For instance, in the United States, cybercriminals zeroed in on Equifax, stealing the personal information of more than 145 million customers. The first repercussion most people thought of concerned the danger of identity theft. But that's just the beginning. Because of all the sensitive information Equifax housed, the hack was a blow to all organizations, including financial services companies. The Equifax breach and the 2015 Anthem breach before it rendered the Social Security number virtually useless as a trusted identifier throughout our economy. Social Security numbers used to be the gold standard, on which banks, credit card companies and others in the financial sector relied heavily for proof of identity. Without a secure identifier, assets become vulnerable, making the need for a digital ID much more urgent.

## ATTACK METHODS AND INNOVATION

The attack methods cybercriminals use against the financial sector are similar to those used for other enterprises and organizations. Ransomware is the fastest growing cybercrime tool, with more than 6,000 online criminal marketplaces selling products and services, and ransomware-as-a-service is growing in popularity. Phishing attacks remain popular, and cybercrime-as-a-service is a big business. The dark web (the part of the World Wide Web that is accessible only by means of special software, allowing users and

website operators to remain anonymous or untraceable) offers buyers web injections, exploit kits and botnet rentals, among other tools. In some cases of ransomware, there really is no ransom that can be paid; data is simply encrypted with no way to retrieve it. This is a frightening type of cyber-attack, particularly for banks that remember the great depression of the 1930s.

There's been a lot of talk about cybercriminals innovating, and that is certainly accurate. With any new technology, there are uses for good and for bad. For instance, banks are using artificial intelligence and machine learning to enable advanced analytics to better serve and protect customers, but the sharpest cybercriminals also understand how to use it. Likewise, Amazon, Microsoft, Google and others are offering cloud technologies that can cut costs and make it easier to implement solutions, but customers don't always have the security part figured out. If companies put all their data in the cloud but don't protect it, they actually might be worsening their security posture. Our customers report that cybercriminals are also taking advantage of big data and advanced analytics for amassing and analyzing stolen information.

Yet while we know that cybercriminals have innovative tools in their arsenal, we haven't seen much of it yet because the old methods are still working. The exploits we see are more commoditized, and that fits with what we know about cybercriminals: They'll do only what they have to do to get a result, no more. If tried and true tactics like phishing are still working, why spend money to purchase a more sophisticated technique? We're seeing some new uses of exploits of WannaCry and Not Petya, and they continue to produce results. We also haven't seen a deliberate, sustained, destructive attack – the type that would render the organization inoperable – against a major American bank. This doesn't mean the financial sector has not been greatly impacted, however, as the theft of so much personal information in other hacks has weakened the fabric of the nation's financial infrastructure.

I do want to mention something that qualifies as an attack method, and that's the abuse of social media. Nation states have shown they're capable of interfering with, misdirecting and altering social media content – all of which can cause panic in financial markets. North Korea and Russia could certainly use social media to spread false information about financial conditions and markets, causing volatile markets to respond to fraudulent news. This is another example of evolving platforms such as social media, cloud and mobile offering both new opportunities as well as new means for abuse. We should be mindful that we're fighting a war, and it's very hard to keep up. We're going to need a lot of work by vendors and the government to protect citizens' information and keep major infrastructures such as power, water and finance stable.

## WHAT HAPPENS TO THE DATA?

In 2015, McAfee produced a report on the market for stolen data (The Hidden Data Economy: the marketplace for stolen digital information), finding that stolen financial data is available not only on the dark web but also to anyone with a browser and the means to pay. Payment card information varies in price, depending on the amount of it out there. In 2015, the cost in the U.S. for a payment card number with a card verification value with a bank ID number and date of birth was $15. Today, it's worth approximately $12. PayPal

logins today go for $247 and online banking details for $160, according to the recently published Dark Web Market Price Index. The Index places the cost of purchasing a passport at $62, with the lowest cost stolen credentials being for Spotify – 12 cents to get a login.

Buyers of stolen information have many options, including the geographic source of a credit card and the card's available balance – both of which affect its price. Here's copy from a marketplace advertising its wares, as noted in the McAfee study referenced above:

> We are offering top quality cards. All our cards come with PPis [personal private information] and instructions. You can use them at any ATM worldwide. Our cards are equipped with magnetic strip and chip. Once you purchase, we will email you a full guide on how to safely cash out.

Everything is available on these online marketplaces, including credentials for bank-to-bank transfers and banking logins. As in other marketplaces, there are scams. One seller pitches: "Are you fed up of being scammed, and ripped? Are you tired of scammers wasting your time, only to steal your hard-earned money?" Just as in the legitimate digital marketplace, online forums are full of advice from buyers. Some sellers employ YouTube to advertise their wares. Still other types of data for sale includes access to systems within organizations' trusted networks. The types of entry vary, from very simple direct access (such as login credentials) to those that require a degree of technical competence (such as vulnerabilities).

Today, the monetization of stolen data has become easier due to the increased widespread use of digital currencies. According, again, to the McAfee-CSIS study on the Economic Impact of Cybercrime, anonymizing services like the "TOR" network and digital currencies have created an environment that gives cybercriminals both an arsenal and a sanctuary. TOR – free software that enables anonymous communication – has greatly enabled the expansion of cybercrime by allowing cybercriminals to hide their identities through a digital medium, further complicating law enforcement tracking efforts. Ransomware payments, for example, have been made more convenient and less traceable by crypto (digital) currency.

I want to emphasize, however, that these black markets represent uses of stolen data that are known – and most of these apply to criminals who hack for financial gain. Even more concerning are the evolving nation state hackers, who often are not putting the stolen data up for sale. The uses they have in mind go beyond simple financial gain, and that's the more worrisome part.

**PREPAREDNESS**

Our customers tell us that the three biggest problems they have are 1) dealing with conflicting regulations, 2) a constantly changing and evolving technology landscape and 3) the growing sophistication of cyber attackers. They also have to deal with cybersecurity tools that often don't work well with each other. The lack of interoperability among cybersecurity solutions limits their ability to exchange threat data on a rapid basis and creates seams of access for hackers. For our customers and also for McAfee and many

other organizations, including the federal government, a fourth problem is the insufficient supply of cybersecurity talent: There are simply too few qualified operators and professionals to enable organizations to stay on the top of their cybersecurity game.

The NIST Cybersecurity Framework provides a valuable roadmap for organizations of all sizes to evaluate their risk and see where their vulnerabilities are. We commend the U.S. government for enabling this partnership that has improved the security posture of many critical infrastructure industries. Likewise, compliance with Europe's General Data Protection Regulation (GDPR) will have a significant impact on improving both the security and privacy practices of those U.S. companies that collect data from European Economic Area residents. GDPR protects personal data in both administrative and technical manners, requiring anyone handling the data to record their uses and make sure that they are securing it.

Most major financial institutions are prepared for major cybersecurity attacks with the potential to produce system-wide failure. They have plans in place and are engaging actively in cyber sharing groups, in collaboration with the Department of Homeland Security (DHS), the Office of the Comptroller of the Currency (OCC) and the Federal Reserve. They know what they'll do first to identify and respond to a nation-state attack against economic critical infrastructure.

Our customers know that major attacks are possible. They don't know if they're imminent. So far, we haven't seen much use of the personal information stolen from Equifax and others, but the financial sector is ready and waiting. As good a job as institutions like Bank of America and US Bank are doing, they can't be expected to deter a nation state on their own. These companies value the partnership they have with the federal government in fighting cybercrime, and they look forward to having agencies such as DHS improve their cybersecurity capabilities.

Following are recommendations for ways the U.S. government can help in the constant battle against cybercrime.

## POLICY RECOMMENDATIONS

**Make the Social Security Number (SSN) Secure:** The venerable nine-digit number first appeared as an identifier in 1936. It has become the de facto national identifier, a federal credential that people use for a range of both governmental and commercial purposes – uses for which it was never designed. Not surprisingly, the SSN is easy to guess, falsify or duplicate, and has become a premier target for cybercriminals. SSNs are sold in bulk in the cybercrime black market for as little as one dollar. Once stolen, the SSN cannot be reissued or replaced, making it a weak foundation upon with to build identity.

The steady stream of major breaches where consumers' SSNs were stolen, the most recent being 145 million stolen from Equifax, creates a compelling opportunity for change. Policymakers need to modernize the Social Security Number system. A good start is to determine what digital technologies offer strong security to create renewed confidence in the Social Security credential. A private sector eco-system of trusted identity management could then be built upon the new foundation of a modern, digitally secure SSN.

**Enhance Cyber Threat Information Sharing:** Although the financial services sector is a leader in information sharing, particularly in comparison to other sectors that are just now developing their own information sharing capabilities, the government can do more to help the financial services industry, and indeed, all industries, get the full benefit of cyber threat information sharing. McAfee believes that U.S. government efforts such as the DHS Automated Indicator Sharing (AIS) capability are useful but do not go far enough. There is a need to move beyond simple indicators supplied via AIS and provide a means to allow enrichment of the shared information.

Organizations need the ability to proactively collect, analyze and disseminate actionable intelligence. They need to consistently and proactively collect information and investigate it in an effort to show attribution. The government should work with the private sector to further evolve the way cyber threat information is represented, enriched and distributed in a timely fashion. Doing so will help create a high-functioning ecosystem of information sharing that enables the public and private sectors to compete with global networks of sophisticated hackers.

**Implement Security and Privacy by Design:** Adding or 'bolting on' security features to a system, network or device after it's already up and running has inherent weaknesses and inefficiencies, particularly in the financial sector, where companies are constantly being attacked. Policymakers should champion security and privacy by design to help incent broad adoption by the information and communication technology (ITC) ecosystem that supports all critical infrastructure sectors, including financial services. Proper protection of personal data in products needs to become an expectation throughout all data-centric industries.

**Promote Cybersecurity Interoperability:** Policymakers can help encourage the cybersecurity industry to continue to evolve by offering customers more solutions that benefit from an open platform model. An open platform is an architecture that makes it easier to deploy and manage a broad set of capabilities, not a business model dictating who and how others can participate. The broad set of capabilities, for instance, on Salesforce would not be possible on a closed platform.

Open cybersecurity platforms increase the rate and breadth of innovation by lowering development costs across the ecosystem. This helps leverage the power of the entire cybersecurity community to help stop the majority of unknown malware, correlate events across the broadest set of threat intelligence and produce compliance solutions appropriate for the largest population of customers. We support driving broad-based industry collaboration and adoption, partnering with standards groups to drive change toward open interfaces and allowing security products to more seamlessly integrate out of the box. We urge policymakers to reform federal procurement rules to enable faster uptake of cybersecurity solutions, particularly those based on open platforms. If procurement rules encouraged open platforms, moving the market to more standardized, open, and interoperable solutions, this alone would improve the security posture of our entire ITC ecosystem.

**Pass National Breach and Security Legislation:** Financial institutions are currently required to comply with the Gramm-Leach-Bliley data protection rules, and through interagency guidance, address data breach preparedness to protect their customers' data. GDPR requirements will further increase security and privacy protections for international organizations. McAfee supports the ongoing efforts to provide a U.S. federal data breach standard to enhance consumer protection to all Americans and across all sectors.

A federal data breach notification law, if implemented effectively, would provide public benefits by enhancing security and privacy, particularly in less-regulated sectors of the economy. It would support the flexibility of the NIST Cybersecurity Framework and allow organizations to focus on a single set of expectations. A U.S. federal breach law should provide a safe harbor for encrypted data and other cybersecurity protections. The ideal law would encourage good corporate behavior and incent companies to implement strong end-to-end cybersecurity programs. The U.S. federal law should be based on a technology-neutral framework that encourages effective, risk-based security strategies to protect personal information. The law should set simple procedural standards for breach notification (e.g., timing, what must be stated, who must be notified, etc.).

Requirements for federal preemption of state law, however, must be carefully considered. Pre-emption must not stifle innovation or weaken protections to those in states with strong data breach and data protection laws. While eliminating the patchwork of existing laws would provide the benefit of uniformity and additional legal certainty, this goal should not be accomplished by lessening existing strong and effective state laws.

## CONCLUSION

The largest and most sophisticated companies in the financial services sector are at the top of their game in cybersecurity, particularly in comparison to smaller financial services companies and other industry sectors that have lagged in investing in the strategies, processes, people and technology needed to keep up with new threats and attackers. Thank you for giving me the opportunity to suggest ways the government can step up its cybersecurity game for the benefit of all financial services companies and consumers. I look forward to answering your questions.