Opening Remarks of FTC Chairwoman Edith Ramirez
Fall Technology Series: Ransomware
Washington, D.C.
September 7, 2016

Good afternoon and welcome to the Federal Trade Commission's workshop on ransomware. This is the first in a series of events that we are hosting this fall to examine the consumer protection implications of new and evolving technologies.

From the earliest days of the Internet, criminals have used an array of tactics to trick consumers into downloading malware, spyware, and other unwanted software onto their computers and devices. This software makes our computers more vulnerable to viruses, allows scammers to monitor consumers' online activity, and provides a pathway for them to steal personal information, which they can then use to perpetrate fraud.[1]

In recent years, criminals have found a new business model for this kind of malicious activity in the form of ransomware. This type of malware infiltrates a computer system and uses tools like encryption to hold valuable data "hostage" in exchange for a ransom. By charging victims for the return of their data, criminals have created a new market for personal information, making ransomware even more profitable than other scams. In fact, recent reports describe ransomware as the most profitable malware scam in history.[2] And no one is immune – individual consumers, government agencies, and entities of all types and sizes have been targets.

The attack on Hollywood Presbyterian Medical Center in Southern California earlier this year, the first in a string of high profile attacks on health care organizations, highlights the

---

[1] FED. TRADE COMM'N, Consumer Information on Malware, *available at* https://www.consumer.ftc.gov/articles/0011-malware.
[2] Tom Risen, *Ransomware Is the Most Profitable Hacker Scam Ever*, U.S. NEWS & WORLD REPORT, July 27, 2016, *available at* http://www.usnews.com/news/articles/2016-07-27/cisco-reports-ransomware-is-the-most-profitable-malware-scam-ever.

challenges ransomware poses. The perpetrators took out the hospital's entire network for more than a week, leaving staff without access to email and certain critical patient data. The malware crippled the hospital's emergency room systems and other computer systems necessary for patient care, and forced hospital staff to log medical records with pen and paper. Ultimately, the hospital paid a ransom of 40 bitcoins, or $17,000, to restore its operations.[3]

Another attack in March disabled MedStar Health's computer systems, denying access to email and patient records at ten hospitals in the Washington, D.C. region for nearly two weeks. Given these kinds of high profile incidents, it is not surprising that ransomware is among the most troubling cyberthreats.[4]

Today, I would like to highlight some of the key challenges associated with ransomware and the important role that businesses and the FTC play in combatting this growing threat.

I. Overview of the Ransomware Threat

The ransomware threat is becoming more pernicious because of the dramatic increase in the number of attacks, the lucrative nature of the threat, the many ways in which criminals are infecting targets, and the potential for causing significant harm to both consumers and businesses alike.

First, the spate of ransomware incidents are increasing at an alarming rate. According to the Department of Justice, ransomware attacks have quadrupled in the last year alone, averaging 4,000 a day.[5] The financial motivation for ransomware attacks suggests that the threat is

---

[3] Richard Winton, *Hollywood hospital pays $17,000 in bitcoin to hackers; FBI investigating*, L.A. TIMES (Feb. 18, 2016), *available at* http://www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html.

[4] *See, e.g.*, PONEMON INST., SIXTH ANNUAL BENCHMARK STUDY ON PRIVACY & SECURITY OF HEALTHCARE DATA 2 (May 2016), *available at* http://www.ponemon.org/blog/sixth-annual-benchmark-study-on-privacy-security-of-healthcare-data.

[5] *See* DEP'T OF JUSTICE ET AL., HOW TO PROTECT YOUR NETWORKS FROM RANSOMWARE 2, *available at* https://www.justice.gov/criminal-ccips/file/872771/download.

unlikely to go away any time soon. According to data from Cyence, Inc., typical ransomware payments range from $500 to $1,000, but some criminals have demanded as much as $30,000.[6]

The perpetrators of ransomware attacks are also using a wide range of tactics to lure their targets into downloading malicious software. They used to rely on spam e-mail to deliver ransomware. But as spam filters have grown better at blocking these messages, some attackers have turned to spear phishing targeting specific individuals or organizations.[7] According to some reports, 93% of all phishing emails now contain some variant of ransomware.[8] Others avoid e-mail altogether by implanting malicious code on seemingly legitimate websites or by exploiting unpatched vulnerabilities on servers.[9] For instance, one version of ransomware called "SamSam" exploits a web application server vulnerability found in over 3.2 million machines used mainly by schools, local governments, and aviation companies.[10] As some of today's panelists will explain, cybercriminals continue to devise new and creative methods for spreading this malware.

The harm caused by ransomware attacks is also rising. Attacks targeting consumers capitalize on the fact that victims are likely to pay to prevent losing important documents or irreplaceable personal items like family photos. And some new forms of ransomware specifically target consumers' mobile devices, rendering them completely inoperable.

Attacks targeting businesses can also impose significant costs. Even beyond the tremendous monetary losses, attacks on businesses can also have devastating effects on

---

[6] Robert McMillan, *In the Bitcoin Era, Ransomware Attacks Surge*, WALL ST. J., Aug. 19, 2016, *available at* http://www.wsj.com/articles/in-the-bitcoin-era-ransomware-attacks-surge-1471616632.
[7] *See* FED. BUREAU OF INVESTIGATION, Incidents of Ransomware on the Rise: Protect Yourself and Your Organization (April 29, 2016), *available at* https://www.fbi.gov/news/stories/incidents-of-ransomware-on-the-rise.
[8] Maria Korolov, 93% of phishing emails are now ransomware, CSO (June 1, 2016), www.csoonline.com/article/3077434/security/93-of-phishing-emails-are-now-ransomware.html.
[9] *See* FED. BUREAU OF INVESTIGATION, *supra* note 7.
[10] *See* Katherine Noyes, Schools put on high alert for JBoss ransomware exploit, CSO ONLINE (April 18, 2016), http://www.csoonline.com/article/3057204/security/schools-put-on-high-alert-for-jboss-ransomware-exploit.html.

consumers. For example, ransomware attackers may be able to steal extremely sensitive consumer information, such as medical information, financial account numbers, and the contents of private communications, some of which may be sold on the dark web. And, by shutting down companies' ability to operate, attackers can deny essential and even life-saving services to consumers, such as access to medical records in an emergency.

In light of the significant risk of harm that ransomware poses, as well as the increase in the number and sophistication of attacks, we are eager to expand our understanding of this growing threat.

II. Role of the Federal Trade Commission

As an agency that has long addressed the harm caused by malware, including the challenges it poses to securing consumer data, the FTC plays a unique role in this area. For nearly a decade, we have worked with other agencies and provided guidance to both consumers and businesses on how to best protect their computers and networks. For example, in 2014, the FTC, along with the FBI and other agencies, issued warnings to businesses about the threat posed by Cryptolocker, an early form of crypto-ransomware, and recommended that businesses proactively defend against it by backing up data, securing network settings, and training employees. These tips are no less relevant today.

The FTC's privacy and data security programs also stress the importance of good cyber hygiene and network security, which can help prevent ransomware attacks. We have brought approximately 60 enforcement actions against companies that have failed to reasonably secure consumer data on their networks. Through our enforcement, we aim to ensure that companies make truthful representations about their privacy and security practices and that they provide reasonable security for consumer information.

One component of reasonable security is that companies have procedures in place to address vulnerabilities as they arise, including malicious software. A company's unreasonable failure to patch vulnerabilities known to be exploited by ransomware might violate the FTC Act. For example, in a recent case against device manufacturer ASUS, we alleged that the company's pervasive security bugs left the company's routers vulnerable to malware, and that attackers exploited these vulnerabilities to reconfigure consumers' security settings and take control of consumers' web activity. We also alleged that the company did not address these security vulnerabilities in a timely manner and did not notify consumers about the risks posed by their vulnerable routers.

In another case against Wyndham Worldwide, we alleged that hackers infiltrated the network of a Wyndham franchisee, navigated to the company's network and the networks of other franchisees, and placed memory-scraping malware on the franchisees' servers. We alleged that these hackers exploited Wyndham's lax security to steal sensitive consumer data from dozens of Wyndham franchisees.

As these cases illustrate, businesses play a critical role in ensuring that they adequately protect consumers' information, particularly as security threats like ransomware escalate.

III. Overview of Ransomware Workshop

As we continue to learn more about the impact and scope of ransomware attacks, we find ourselves facing a number of questions. For example, are there steps consumers and businesses should be taking to reduce the risk of ransomware or decrease its impact? What can be learned from criminal law enforcement's efforts to combat these attacks? If you fall prey to ransomware, should you pay the ransom? These are just a few of the questions that we will attempt to answer during today's workshop. My hope is that this discussion will provide valuable insight into the

challenges surrounding the ransomware threat, and practical advice on how to meet those challenges.

Our aim is that you leave today's workshop with a better understanding of the threats posed by ransomware, the vectors that attackers use to infect systems, and the tools that consumers and businesses can use to safeguard their data. And in the months ahead, we hope you will continue to work with us to help address this challenging issue.

Before we turn to the first panel, I would like to thank FTC staff from our Division of Privacy and Identity Protection, Division of Marketing Practices, and Office of Technology Research and Investigation for their work in organizing today's workshop – in particular, Ben Rossen, Will Maxon, Steve Wernikoff, and Joe Calandrino – and all of our speakers who are here today to share their insights on this important issue.

Thank you for joining us.