ROBERT MENENDEZ
NEW JERSEY

COMMITTEES:
BANKING, HOUSING, AND URBAN AFFAIRS
FINANCE
FOREIGN RELATIONS

United States Senate

WASHINGTON, DC 20510–3005

528 SENATE HART OFFICE BUILDING
WASHINGTON, DC 20510
(202) 224-4744

ONE GATEWAY CENTER
11TH FLOOR
NEWARK, NJ 07102
(973) 645-3030

208 WHITE HORSE PIKE
SUITE 18-19
BARRINGTON, NJ 08007
(856) 757-5353

October 31, 2017

The Honorable Jamal El-Hindi
Acting Director
Financial Crimes Enforcement Network
1500 Pennsylvania Avenue, NW
Washington, DC 20220

Dear Acting Director El-Hindi:

As you know, the recent Equifax data breach exposed the personally identifiable information of more than 143 million people. Shortly after news of the data breach broke, reports surfaced that the perpetrators were demanding 600 bitcoin in ransom.[1] These reports raise serious concerns about the role of bitcoin in future breaches. As such, I write to request information on the Financial Crimes Enforcement Network's (FinCEN) oversight and engagement on the use of digital currency in ransomware attacks.

According to research from New York University ("NYU") and Google, "ransomware" is quickly becoming a multi-million dollar business.[2] Ransomware is malware that locks your keyboard or computer to prevent you from accessing your data until you pay a ransom, usually demanded in bitcoin. Ransomware is quickly becoming profitable criminal enterprise. Notably, the NYU and Google research team found a sharp increase in the number of cases in the second quarter of 2016.[3] Where ransom was paid, 95 percent were paid through BTC-E, a Russian-operated bitcoin exchange platform.[4] In sum, ransomware victims paid out more than $25 million during a two year period from 2015-2016.[5] Just this past June, hackers withdrew $143,000 worth of bitcoin from an online wallet following the WannaCry ransomware attack that locked down files throughout the United Kingdom, including the National Health Service.[6] These attacks have clear global repercussions for security and privacy.

Because of the anonymous nature of bitcoin transactions, the digital currency is an ideal choice for criminals. Law enforcement is deliberately and steadily making strides in tracing the movement of online criminals. For example in 2013, the federal government arrested Ross Ulbricht, the founder of a major underground drug market, and seized more than $3.5 million worth of bitcoin.[7]

---

[1] http://mashable.com/2017/09/08/equifax-hackers-bitcoin-ransom/#5a2.xxXvSkq4
[2] https://www.usatoday.com/story/tech/2017/07/25/google-ransomware-tracking-bitcoin/506560001/
[3] *Id.*
[4] *Id.*
[5] https://www.theverge.com/2017/7/25/16023920/ransomware-statistics-locky-cerber-google-research
[6] https://www.cnbc.com/2017/08/03/hackers-have-cashed-out-on-143000-of-bitcoin-from-the-massive-wannacry-ransomware-attack.html
[7] https://www.washingtonpost.com/news/the-switch/wp/2017/05/15/what-you-need-to-know-about-bitcoin-after-the-wannacry-ransomware-attack/?utm_term=.974900a17dac

The Internet presents a formidable obstacle to law enforcement, with new bad actors constantly replacing those who have been apprehended. Nonetheless, I have a responsibility to do everything within my power to remain vigilant and prevent harm wherever possible. I am aware FinCEN is already working to combat financial crimes that utilize currency exchanges.[8] However, given the recent uptick in ransomware crimes, please provide responses to the following requests and questions no later than November 30:

(1) An update on what proactive steps FinCEN is taking to prevent criminals from gaining an advantage by using digital currency and digital currency exchanges;

(2) Does FinCEN have both sufficient authority and resources to effectively track the illegal use of digital currency in ransomware attacks? Specifically, is the 2013 FinCEN guidance on virtual currency in need of an update?[9]

(3) In what capacity, if at all, is FinCEN engaged with the Board of Governors of the Federal Reserve System to ensure that use of digital currencies does not interfere or create a threat to the banking system, economic activity, and financial stability?

(4) What steps can FinCEN take to ensure that hackers are not emboldened to steal consumer data knowing that digital ransom is easily paid?

The severity of the damage inflicted by largescale data breaches demands our immediate attention. Left ignored, this threat is likely to get worse before it gets better.

Sincerely,

Robert Menendez
United States Senator

Cc: The Department of Justice

---

[8] https://www.fincen.gov/news/news-releases/fincen-fines-btc-e-virtual-currency-exchange-110-million-facilitating-ransomware

[9] https://www.fincen.gov/news/news-releases/fincen-issues-guidance-virtual-currencies-and-regulatory-responsibilities