RON WYDEN
OREGON

CHAIRMAN OF COMMITTEE ON FINANCE

221 DIRKSEN SENATE OFFICE BUILDING
WASHINGTON, DC 20510
(202) 224-5244

United States Senate

WASHINGTON, DC 20510-3703

COMMITTEES:
COMMITTEE ON FINANCE
COMMITTEE ON BUDGET
COMMITTEE ON ENERGY & NATURAL RESOURCES
SELECT COMMITTEE ON INTELLIGENCE
JOINT COMMITTEE ON TAXATION

December 15, 2015

Director James B. Comey
Federal Bureau of Investigation
U.S. Department of Justice
935 Pennsylvania Avenue, NW
Washington, DC 20535-0001

Dear Director Comey,

I write today with great concern about the growing criminal practice of hacking Americans' devices, encrypting their personal information and holding it for ransom through software commonly referred to as ransomware. The FBI has reported that common ransomware known as Cryptowall has led to nearly 1,000 complaints over a 14-month period, with victims reporting losses totaling more than $18 million.

Victims of ransomware attacks are reporting payments between $200 and $10,000 to get their personal or business-related data back. These unexpected costs could be a financial disaster for a family or small business. Not only are victims hit in the wallet, they also are burdened with the additional costs of replacing their breached hardware, bringing legal action and updating security for their systems. Not to mention the implications of a business' responsibilities to its employees or customers. Even more worrisome is the possibility that they become a target susceptible to future attacks, just by paying the ransom.

In order to better understand how the FBI is tackling the problem, I would like answers to the following questions;

1. FBI officials have been quoted as saying the Bureau often advises people "just to pay the ransom." Is this an accurate description of FBI policy with respect to ransomware?
2. Media reports indicate authorities in the Netherlands, working with an independent cybersecurity firm, effectively disabled and decrypted two popular ransomware products. What public or private options are available to assist U.S. victims of encryption hacking?
3. Media reports largely attribute encryption hacking attacks to foreign organized crime groups. Is this accurate?
4. In the nearly 1,000 Cryptowall-related complaints that the FBI has reported on, for what percentage has the FBI have identified a suspect?
5. If the FBI is unable to track the source of the attacks, what is it doing with its substantial experience and abilities in financial forensics to trace the payments and stop these criminal groups from profiting off their scams?'
6. Does the FBI require additional tools or authorities to assist in tracking ransom payments from victims to cyber criminals?

911 NE 11TH AVENUE
SUITE 630
PORTLAND, OR 97232
(503) 326-7525

405 EAST 8TH AVE
SUITE 2020
EUGENE, OR 97401
(541) 431-0229

SAC ANNEX BUILDING
105 FIR ST
SUITE 201
LA GRANDE, OR 97850
(541) 962-7691

U.S. COURTHOUSE
310 WEST 6TH ST
ROOM 118
MEDFORD, OR 97501
(541) 858-5122

THE JAMISON BUILDING
131 NW HAWTHORNE AVE
SUITE 107
BEND, OR 97701
(541) 330-9142

707 13TH ST, SE
SUITE 285
SALEM, OR 97301
(503) 589-4555

HTTP://WYDEN.SENATE.GOV

With this problem becoming increasingly widespread, the FBI should explore all legal options for stopping the successful use of ransomware. Not only should these efforts focus on cyber criminals conducting encryption attacks, they should also target the ransom payments from victims to cyber criminals.

As we continue to live in a global economy driven by Internet communications, the need to stop bad actors becomes more important every day. Thank you in advance for your response to my request.

Sincerely,

Ron Wyden
U.S. Senator