TIM JOHNSON, SOUTH DAKOTA, CHAIRMAN

JACK REED, RHODE ISLAND
CHARLES E. SCHUMER, NEW YORK
ROBERT MENENDEZ, NEW JERSEY
SHERROD BROWN, OHIO
JON TESTER, MONTANA
MARK WARNER, VIRGINIA
JEFF MERKLEY, OREGON
KAY HAGAN, NORTH CAROLINA
JOE MANCHIN, WEST VIRGINIA
ELIZABETH WARREN, MASSACHUSETTS
HEIDI HEITKAMP, NORTH DAKOTA

MICHAEL CRAPO, IDAHO
RICHARD C. SHELBY, ALABAMA
BOB CORKER, TENNESSEE
DAVID VITTER, LOUISIANA
MIKE JOHANNS, NEBRASKA
PATRICK J. TOOMEY, PENNSYLVANIA
MARK KIRK, ILLINOIS
JERRY MORAN, KANSAS
TOM COBURN, OKLAHOMA
DEAN HELLER, NEVADA

CHARLES YI, STAFF DIRECTOR
GREGG RICHARD, REPUBLICAN STAFF DIRECTOR

United States Senate
COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS
WASHINGTON, DC 20510–6075

October 21, 2014

The Honorable Jacob Lew
Secretary
U.S. Department of the Treasury
1500 Pennsylvania Avenue, NW
Washington, DC 20220

The Honorable Janet Yellen
Chair
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue, NW
Washington, DC 20551

The Honorable Martin Gruenberg
Chairman
Federal Deposit Insurance Corporation
550 17th Street, NW
Washington, DC 20429

The Honorable Thomas Curry
Comptroller
Office of the Comptroller of the Currency
400 7th Street, SW
Washington, DC 20219

The Honorable Debbie Matz
Chair
National Credit Union Administration
1775 Duke Street
Alexandria, VA 22314

Dear Secretary Lew, Chair Yellen, Comptroller Curry, Chairman Gruenberg, and Chair Matz:

Over the past decade, cybersecurity has become a foremost national priority for both the government and the private sector. Our networks and information systems are under attack from a wide range of actors, including sophisticated criminal organizations, nation-states, and "hacktivists," who commit cyberattacks for a variety of reasons. Cyberattacks come in many different forms, including distributed denial service attacks against websites, point-of-sale attacks against merchants, malware attacks to infiltrate secure systems, phishing scams, and many more.

As Chairman and Ranking Member of the U.S. Senate Committee on Banking, Housing, and Urban Affairs, we are particularly concerned with the safety and integrity of the U.S. financial system, especially as it pertains to Americans' personal financial information. The economic impact of cyberattacks is staggering. A recent Center for Strategic and International Studies report projected global economic losses of up to $575 million annually in the U.S. alone. An earlier report cited by President Obama estimated losses of $1 trillion just from intellectual property theft by cyberattacks over the previous year. Financial institutions are a particularly lucrative target. Many find themselves under constant attack, with some spending up to $250 million per year on cybersecurity.

According to Larry Zelvin, Director of the National Cybersecurity and Communications Integration Center at the Department of Homeland Security (DHS), of the sixteen critical infrastructure sectors, "finance probably wins the cybersecurity threat award. . . . [The industry is] a massive target . . . because [it is] where the money is." The Office of the Comptroller of the Currency recently noted in its Semi-Annual Risk Perspective for U.S banks that [cyberattacks and breaches] are a leading operational risk and that "recurring security breaches at retail merchants highlight the interdependencies in today's payment systems…there is concern that criminals will transition from disruptive attacks to attacks that are intended to cause destruction and corruption."

Over the past year, we have seen a notable increase in the frequency and scope of data breaches at U.S. companies, which often involve the theft of customers' financial and other personal information. According to a recent study conducted by the Ponemon Institute, 43 percent of companies experienced a breach in the last year, up from 33 percent the prior year, and 60 percent reported a breach in the last two years. These numbers likely underestimate the magnitude of the current threat, as many breaches occur undetected. In the words of former FBI Director Robert Mueller, "There are only two types of companies: those that have been hacked, and those that will be. Even that is merging into one category: those that have been hacked and will be again." Earlier this month, JPMorgan Chase, the nation's largest bank by assets, announced that personal information from 76 million households and 7 million small businesses had been compromised, one of the largest corporate breaches in history. Additional reports indicate that at least a dozen financial companies were targeted by the same hacker group. Ensuring that customer information is secure is essential to the integrity of the financial system. Furthermore, as new forms of payment become increasingly popular, strong data security will take on even greater importance.

While we recognize that federal agencies have heightened their attention to cybersecurity issues, we are writing to seek more information on the role your agency or Department is playing to protect our financial system from cyberattacks. Please also respond to the following questions to the extent they are applicable to your agency or Department.

First, what is your agency's or Department's process for acquiring information on potential or occurring cyberattacks and passing information to the financial services sector in a timely manner? What obstacles and/or legal restrictions hinder information sharing? Specifically, as the financial services sector's Sector-Specific Agency, Treasury has a number of responsibilities described in Presidential Policy Directive 21 and Executive Order 13636. What actions is Treasury taking to fulfill those responsibilities?

Second, please describe what coordination and interaction each of your agencies and Department have with each other, as well as law enforcement, DHS, and the intelligence community. How would legislative proposals improve or impede your coordination and relationships with other government agencies?

Third, last year, the Financial Stability Oversight Council (FSOC) recommended that regulators devote additional supervisory attention toward cybersecurity. What is the FSOC's role in monitoring cybersecurity risks?

Finally, earlier this year the Federal Financial Institutions Examination Council announced that it is planning cybersecurity and risk-mitigation assessments to help smaller institutions address cybersecurity gaps. Please describe this effort and what particular considerations or risks may exist at institutions of varying sizes.

It is vital that government agencies and private institutions remain vigilant and coordinated in ensuring the safety and security of our networks, especially as it applies to the valuable personal and financial information of American consumers.

Thank you for your attention to this matter.

Sincerely,

Tim Johnson

Mike Crapo