Exhibit 1

FINANCIAL SERVICES ISAC

February 29, 2016

The Honorable Amy Totenberg
United States District Judge
U.S. District Court, Northern District of Georgia
Richard B. Russell Building
75 Ted Turner Drive, Suite 2300
Atlanta, Georgia 30303-3309

Dear Judge Totenberg:

Reconstituting computers compromised by cyber intrusions costs society a significant amount of resources. The Financial Services Information Sharing & Analysis Center (FS-ISAC) provides an estimate of these costs below. These include both the cost of repairing computers and the direct losses incurred by intrusions.

Cost of Reconstituting Computers

Consumers and businesses incur not insignificant labor costs in removing malware from their computers. Commercial banks, for example, have reported that it can require between 1.5 to 3.0 hours to rebuild each compromised computer and return it to use, depending on whether the data is backed up and there is an image that can be restored. Re-imaging the device can double the amount of time required to compete the repair.

The lowest repair cost reported to the FS-ISAC was $75 per machine. However, consumers and small businesses lacking the internal resources to handle these issues often rely on external computer experts, like the Geek Squad. These costs can be as high as $300 per machine. Thus, the cost can range from $75 to $300 per computer, depending on the time needed, as well the use of internal or external resources.

As an example of the high cost of repairs, Microsoft identified 9,691,726 SpyEye infections in 2011 alone. Using the minimal cost estimate (*i.e.*, $75) of removing SpyEye malware from these computers, it would cost at least $726,879,450 in the aggregate to reconstitute affected computers. Needless to say, this is a lower bound.

2011 Losses from SpyEye

The financial sector suffers significant direct costs from cyber intrusions. For example, in 2011 cyber criminals primarily used SpyEye and Zeus to effect successful cyber account takeover attacks. The Federal Deposit Insurance Corporation (FDIC) reported that the SpyEye attacks alone cost commercial banks $64 million.

The American Bankers Association surveyed banks in 2009, 2010, and 2011 on the impact of cyber account takeovers on banks and their corporate customers. In 3% of the

cases, losses were incurred by banks, whereas corporate customers incurred losses in 2% of the cases. Assuming that the $64 million constituted 3% of bank losses, as estimated by the FDIC, the 2% of corporate customer losses amounted to nearly $43 million. Thus, a reasonable estimate of the total losses by banks and their corporate customers from SpyEye and Zeus infections was about $107 million in 2011.

It should be noted that this constitutes a low estimate, because not all cyber account takeover attacks were necessarily reported to the FDIC in 2011. Moreover, cyber security experts agree that the actual losses to banks and their customers were much higher. Nevertheless, it is indicative of the costs imposed by these cyber criminals on financial institutions and their customers.

FS-ISAC Background

The FS-ISAC is a non-profit corporation established in 1999 and funded by its member firms. Its mission is to help ensure the resilience of the global financial services infrastructure and individual firms against acts that could significantly impact the sector's ability to provide services critical to the orderly functioning of the global economy.

With nearly 7,000 members, the FS-ISAC is the largest domestic financial association. It operates in 38 countries, with staff in seven of them. Its membership includes more than 80% of U.S. commercial banks, holding more than 90% of U.S. commercial banking assets—totaling nearly $12 trillion. Broker dealers, credit unions, payment processors, insurance companies, clearinghouses, and exchanges also belong to the FS-ISAC.

Thank you for the opportunity share this important information. Cyber crime constitutes one of the greatest threats to our members, leading us to collaborate regularly with law enforcement and the judicial system. Please do not hesitate to contact me with any questions.

Sincerely,

Brian Tishuk
General Counsel
Financial Services Information Sharing & Analysis Center
btishuk@fsisac.us
12020 Sunrise Valley Drive, Suite 230
Reston, Virginia 20191