

Richard A. Jacobsen (RJ5136)
ORRICK, HERRINGTON & SUTCLIFFE LLP
51 West 52nd Street
New York, New York 10019
Telephone: (212) 506-5000
Facsimile: (212) 506-5151

Gabriel M. Ramsey
(*pro hac vice application pending*)
ORRICK, HERRINGTON & SUTCLIFFE LLP
1000 Marsh Road
Menlo Park, California 94025
Telephone: (650) 614-7400
Facsimile: (650) 614-7401

Attorneys for Plaintiffs
MICROSOFT CORPORATION,
FS-ISAC, INC. and NATIONAL AUTOMATED
CLEARING HOUSE ASSOCIATION

**UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK**

MICROSOFT CORP., FS-ISAC, INC., and
NATIONAL AUTOMATED CLEARING HOUSE
ASSOCIATION,

Plaintiffs

v.

JOHN DOES 1-39 D/B/A Slavik, Monstr, IOO,
Nu11, nvidiag, zebra7753, lexa_Mef, gss, iceIX,
Harderman, Gribodemon, Aqua, aquaSecond, it,
percent, cp01, hct, xman, Pepsi, miami, miamibc,
petr0vich, Mr. ICQ, Tank, tankist, Kusunagi,
Noname, Lucky, Bashorg, Indep, Mask, Enx,
Benny, Bentley, Denis Lubimov, MaDaGaSka,
Vkontake, rfcid, parik, reronic, Daniel, bx1, Daniel
Hamza, Danielbx1, jah, Jonni, jtk, Veggi Roma, D
frank, duo, Admin2010, h4x0rdz, Donsft,
mary.J555, susanneon, kainehave, virus_e_2003,
spaishp, sere.bro, muddem, mechan1zm,
vlad.dimitrov, jheto2002, sector.exploits AND
JabberZeus Crew CONTROLLING COMPUTER
BOTNETS THEREBY INJURING PLAINTIFFS,
AND THEIR CUSTOMERS AND MEMBERS,

Defendants.

Case No. 12-1335

FILED UNDER SEAL

KORMAN, J.

MANN, M.J.

U.S. DISTRICT COURT
EASTERN DISTRICT
OF NEW YORK

2012 MAR 19 AM 8:55

FILED
CLERK

**DECLARATION OF WILLIAM D. JOHNSON IN SUPPORT OF PLAINTIFFS'
APPLICATION FOR AN EMERGENCY TEMPORARY RESTRAINING ORDER AND
ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION**

I, William D. Johnson, declare as follows:

1. I am Vice President and Senior Advisor, Risk Management Policy of the American Bankers Association (“ABA”). I make this declaration in support of Plaintiffs’ Application For An Emergency Temporary Restraining Order And Order To Show Cause Re Preliminary Injunction. Except as otherwise indicated, this declaration is based on my own personal knowledge and my experience and knowledge as Vice President and Senior Advisor, Risk Management Policy and upon the business records of the ABA relating to this role. If called as a witness, I could and would testify competently to the truth of the matters set forth herein.

2. As the largest bank trade association in the United States, ABA represents banks of all sizes and charters within the \$13 trillion banking industry. ABA member banks account for approximately 92 percent of all U.S. banking assets.

3. As Vice President and Senior Advisor, Risk Management Policy, I manage and supervise the ABA’s enterprise risk management, cyber and information security, business continuity and resiliency activities. In that capacity I manage the ABA’s Information Security Working Group, as well as the Association’s Bank Security Committee. These two groups are comprised of bank professionals responsible for their institution’s physical, cyber, and information security programs. I also serve on the board of the Financial Services Information Sharing and Analysis Center (“FS-ISAC”) and the Steering Committee of NACHA’s Internet Council.

4. The FS-ISAC was established in 1999 in response to Presidential Directive 63, which mandated that the public and private sectors share information about physical and cyber security threats and vulnerabilities to help protect the U.S. critical infrastructure. It remains the primary financial services industry forum for public and private sector collaboration on critical security threats facing the sector.

5. NACHA manages the development, administration, and governance of the Automated Clearing House (“ACH”) Network, the backbone for the electronic movement of money and data. The ACH Network provides a safe, secure, and reliable network for direct

account-to-account consumer, business, and government payments. Annually, it facilitates billions of electronic transactions. The mission of NACHA's Internet Council is to advance electronic commerce over open networks by enabling digital business in a straight-through, secure and cost-effective manner.

6. The ABA Routing Number ("RTN"), which was developed by the Association in 1910, was originally designed only to identify check processing endpoints. Today it has evolved to designate participants in ACH, electronic funds transfers and online banking transactions. In the U.S. there are approximately 28,000 active routing numbers currently in use. Every financial institution in the United States must have an RTN to designate the bank from which a physical or electronic negotiable instrument has been drawn.

7. The combination of an ABA RTN and a bank customer's account number can be termed the "credentials" by which a transaction is successfully accomplished. These credentials exist on both sides of all transactions, both the payer and the payee. In legitimate transactions, these credentials ensure that a transaction is successfully accomplished. To the extent that these credentials are stolen, illicit transactions can occur.

8. SPAM – the use of electronic messaging systems to send unsolicited bulk emails – acts as a portal, often attempting to either entice bank customers to directly provide the credentials to their bank accounts or place malicious software on bank customer computers to capture keystrokes that include those credentials.

9. BOTNETs are collections of computers compromised by malicious software used to create and send SPAM.

10. The malicious software sent by a BOTNET associated with SPAM can take control of a bank customers' internet banking session once the customer logs into their internet banking site. Once in control, a criminal, either through computer code or manually, can use that internet banking session to illicitly electronically transmit that customer's funds from their account.

11. Upon information and belief, if these BOTNETS are allowed to continue their operations, more bank customers will become victimized by illicit electronic transactions. These

illicit transactions, if allowed to continue, pose a serious threat to customer confidence and trust in the electronic banking channel.

Bank Customers Are Increasingly Being Victimized By Illicit Electronic Transactions As The Online Banking Channel Grows

12. As the use of checks has diminished, electronic debit card fraud exceeded check fraud for the first time in 2010, reaching \$955 million in the U.S., according to the ABA 2011 Deposit Account Fraud Survey Report. A true and correct excerpt from this Report reflecting these figures is attached as Exhibit 1.

13. In 2010, 96 percent of all banks incurred a financial loss from electronic debit card fraud. The percentage of community banks incurring fraud losses has increased significantly from 2006 to 2010, from 61 percent to 96 percent. A true and correct excerpt from an ABA report reflecting these figures is attached as Exhibit 2.

14. The threat levels for most types of fraud risk against bank accounts continue to increase. The risks that gained most in perceived threat from 2008–2010 were fraudulent ACH originations and online banking fraud. A true and correct excerpt from an ABA report reflecting this activity is attached as Exhibit 3.

15. Banking customers are increasingly dependent on online banking to conduct their banking business. Bank customers now prefer online banking to any other delivery channel, including the branch and the ATM. In 2010, online banking was the preferred banking channel for 62 percent of customers, a significant increase from the 36 percent that indicated online banking was their preferred banking channel in the previous year. A true and correct excerpt from an ABA report reflecting these figures is attached as Exhibit 4.

16. Using SPAM to attempt to steal customer bank credentials is commonly known as PHISHING. PHISHING SPAM purports to come from a trusted source, such as a governmental agency or financial institution. Financial services continue to be the most targeted industry for PHISHING SPAM. In the first half of 2011, almost half of all PHISHING emails purported to come from a financial institution. A true and correct excerpt from a report of the Anti-Phishing Working Group reflecting these facts is attached as Exhibit 5.

17. Successful PHISHING threatens customer confidence and trust in the online banking channel. Javelin Strategy & Research estimates that 11.6 million U.S. citizens were victims of identity theft in 2011, the highest level of reported identity theft since the company began surveying in 2003. According to the survey, in 2011, 4.9 percent of the U.S. adult population, approximately roughly 1 in 20 adults, was affected by identity-related fraud last year.

18. While, under the Electronic Funds Transfer Act and Federal Reserve Regulation E, retail bank customers have a number of legal protections against fraud losses due to identity theft, victims still incur substantial costs. According to the Identity Theft Resource Center, in 2009, victims spent an average of 68 hours and \$741 repairing the damage done by identity theft. Such costs and expenditure of time erode bank customer confidence.

Illicit Transactions Through The Use Of BOTNETS And PHISHING SPAM Are Facilitated Through The Use Of ABA's Domain Name And Rtns Damaging Customer Confidence In Online Banking

19. PHISHING SPAM has been designed to capture customer credentials in the form of the ABA RTN and customer account number. Other PHISHING SPAM has contained ABA routing information that illicitly sends payments to a bank account the attacker controls.

20. In November 2011, emails distributed by BOTNETS purporting to be from "aba.com" were detected over the course of four days. These attacks on banks and bank customers were so large that for every legitimate message sent by the ABA during that time period the BOTNETS distributed 200 malicious messages.

21. In January 2010, BOTNETS distributing emails purporting to be from ABA fraudulently informed recipients that an unauthorized transaction had been charged to their account using their bank card. Clicking on the link contained in the email infected the recipient's computer with malicious software.

22. Beyond the risk of bank customers being defrauded and banks suffering losses, the distribution of PHISHING SPAM creates concern and confusion among bank customers as to the safety of online banking generally.

23. Customer awareness of online threats is increasing dramatically. In 2009, 76

percent of respondents to the RSA 2010 Global Online Consumer Security indicated they were familiar with the threat of phishing, compared to 38 percent in 2007. Despite increased awareness, the number of respondents that indicated they had fallen victim to a phishing attack increased from 5 percent to 29 percent from 2007 to 2009. While awareness of phishing has increased, concern over the phishing threat has remained high. Among those surveyed, 90 percent stated that they were somewhat to very concerned about the threat of phishing.

24. Reducing bank customers' perceptions of risk on the internet is the key determinant in getting bank customers to use online banking. Customers who believe the risk of conducting online banking transactions is low are more willing to conduct those transactions. Their willingness is also more pronounced when they also trust their bank's online banking platform.¹

25. Trust and confidence in online banking is more critical to customers than trust and confidence in other online services. Respondents to the 2009 RSA survey indicated they were somewhat to very concerned (86 percent) with their personal information being accessed or stolen at their online banking site compared to a healthcare (64 percent), government (68 percent) or social networking site (81 percent).

Executed this 18th day of March, 2012

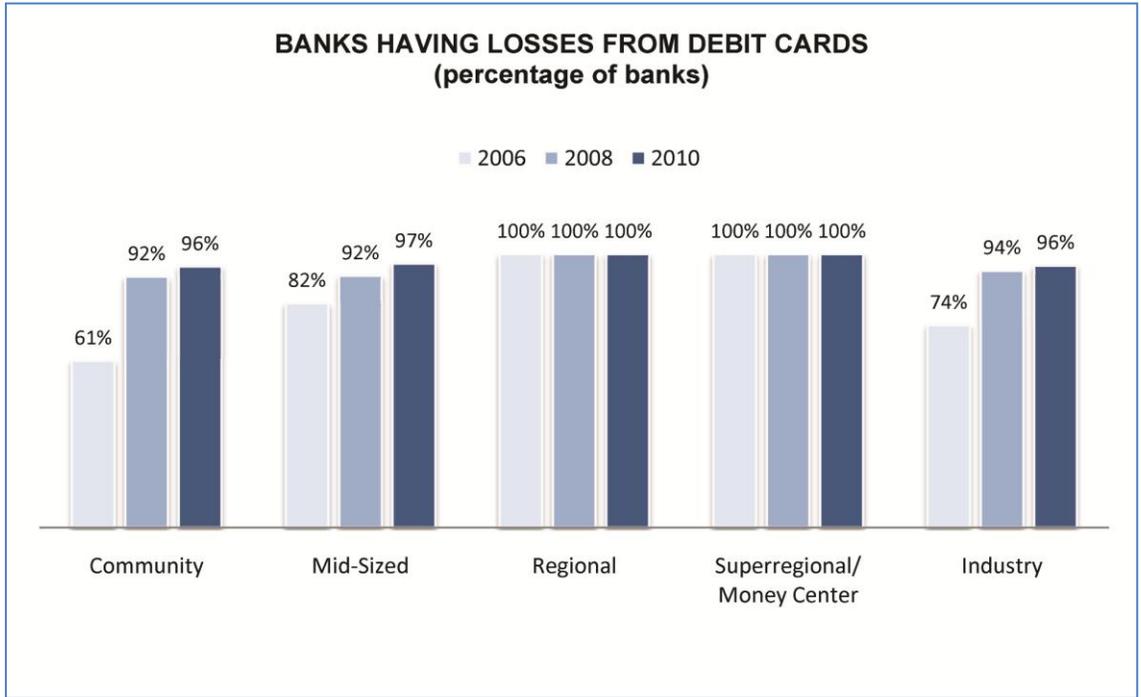


William Johnson

¹ Wong, Loh, Yap, and Bak, (2009), "To Trust or Not to Trust", Journal of Internet Business Issue 6 – 2009; http://jib.debi.curtin.edu.au/iss06_wong.pdf

EXHIBIT 1

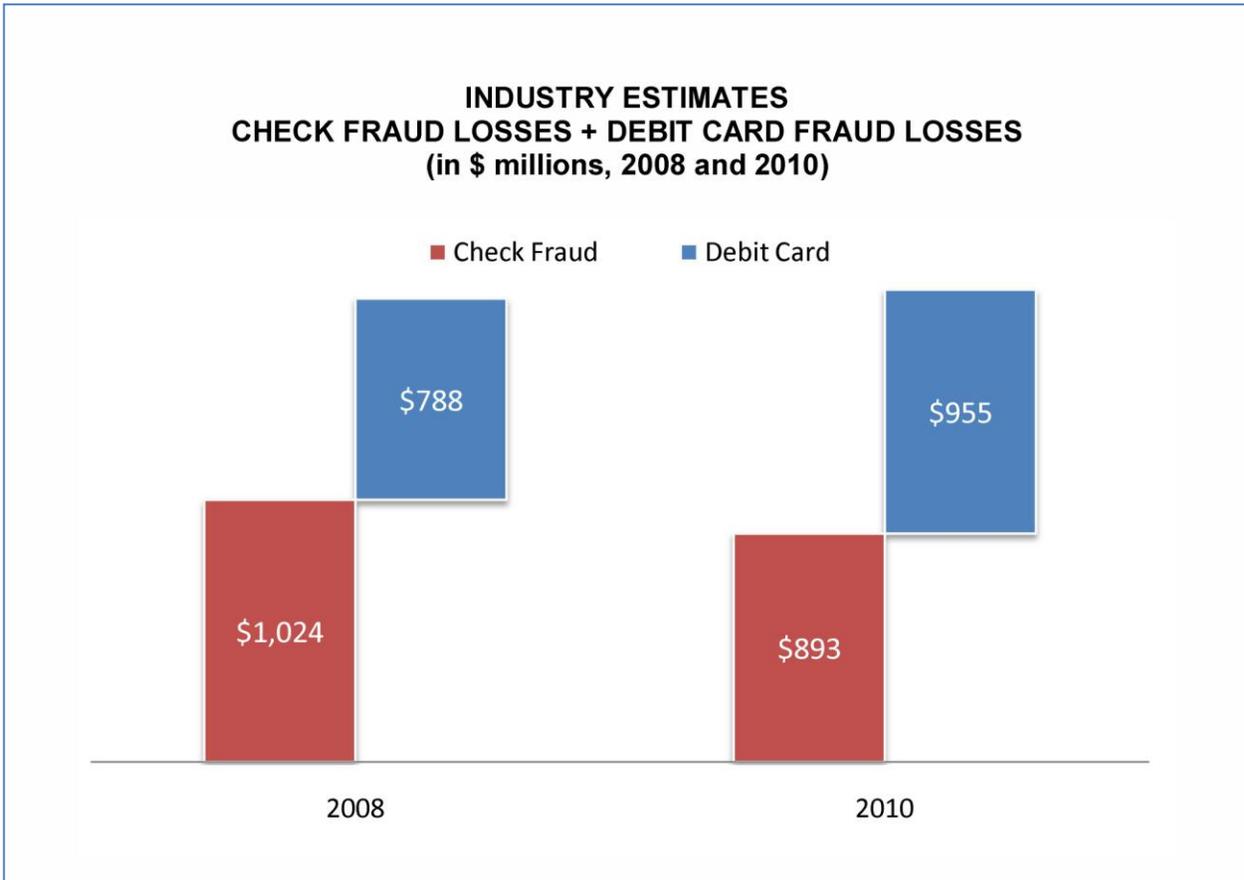
Exhibit 1



Source: American Bankers Association

EXHIBIT 2

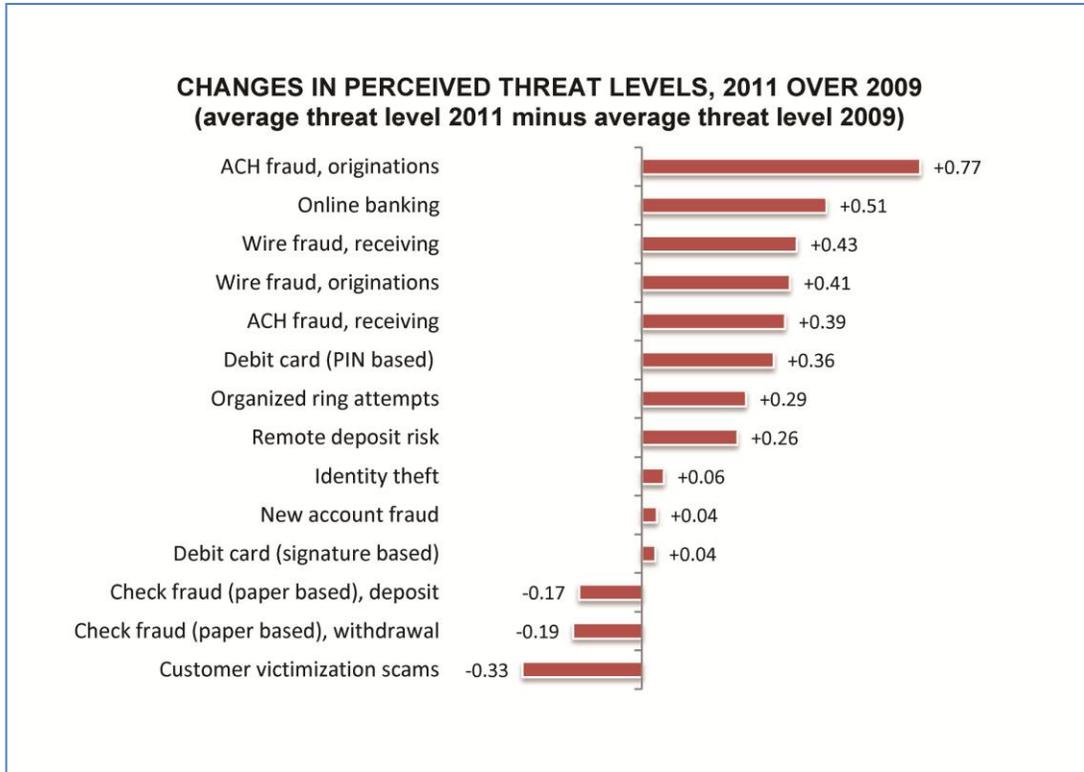
Exhibit 2



Source: American Bankers Association

EXHIBIT 3

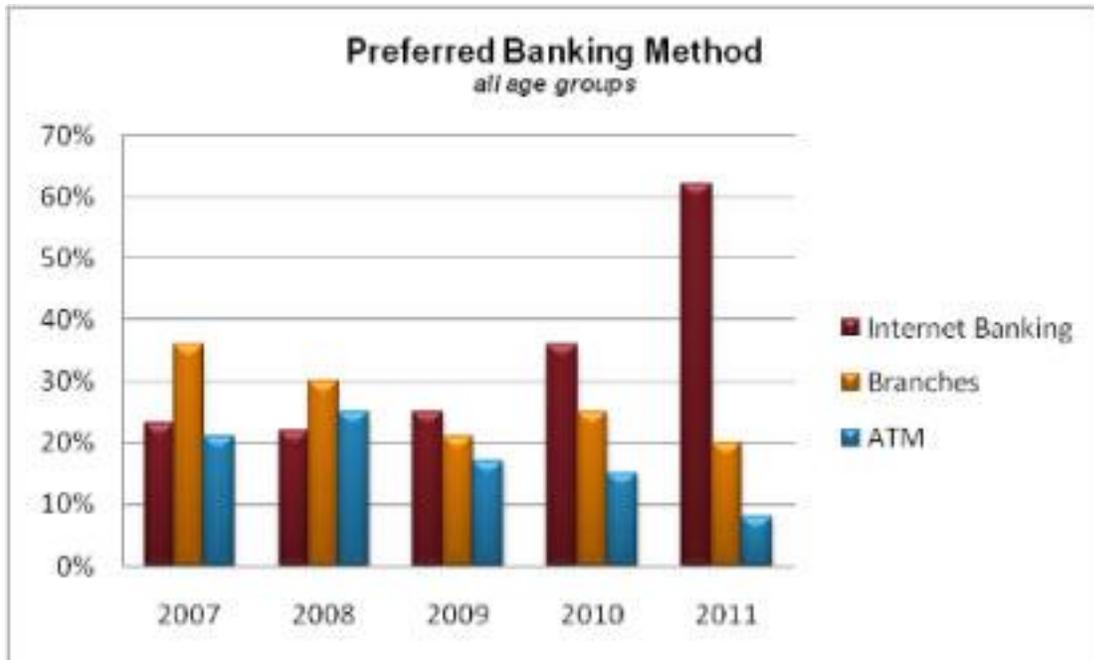
Exhibit 3



Source: American Bankers Association

EXHIBIT 4

Exhibit 4



Source: American Bankers Association

EXHIBIT 5

Exhibit 5

Most Targeted Industry Sectors – 1st Half 2011

Financial Services continued to be the most targeted industry sector in the first half of 2011. Financial Services was previously eclipsed by Payment Services in Q2, 2010, which last eclipsed Financial Services in Q2, 2010, remained the second highest industry sector for targeted attacks. [Data sampling note: the reported retail sector proportion of the target base in H1, 2011 increased markedly to 6.1 percent from 1 percent in Q4, 2010, due to the addition of new data feeds from the Asia Pacific region by APWG research correspondent MarkMonitor.]



Source: Anti-Phishing Working Group