Exhibit A

Exhibit A

Brief Summary of Background and Expertise in the field

Lance James, author of "Phishing Exposed" and a co-author to "Emerging Threat Analysis", has been heavily involved with the information security community for more than 10 years. With over a decade of experience with programming, network security, malware research, cryptography design & cryptanalysis, attacking protocols and a detailed expertise in information security, Lance has provided consultation to numerous businesses ranging from small start-ups, governments, both national and international, as well as Fortune 500's and America's top financial institutions. He has spent the last few years devising techniques to prevent, track, and detect phishing and malware attacks. He is an advisory board member of the Digital PhishNet (a Microsoft/NCFTA/FBI organization), creator of InvisibleNet, a prominent member of the local 2600 and InfraGard chapters, and a Co-Founder of Secure Science Corporation. Lance is actively working with Vigilant as the Director of Intelligence. As a regular speaker at numerous security conferences and being a consistent source of information by various news organizations, Lance James is recognized as a major asset in the information security community.

Specific Summary:

Ever since online fraud attacks against financial institutions became an idea for cyber-criminals to initiate, I have made it my commitment to utilize my information security background to research and understand this problem at an expert level. Within the information security industry, I am referred to by my peers as well as law enforcement (both local and federal) as the "phishing guy". On the phishing and fraud investigation side my investigative work has enabled multiple major busts of these organized groups both in the US and overseas by the FBI. I have been retained both nationally and internationally to train law enforcement, intelligence agencies, and financial institutions, enabling them with leading edge techniques to successfully investigate these ongoing threats.

More specifically, I have been hired by many financial institutions to assist in prevention, mitigation, reconnaissance, remediation and forensic investigations of fraudulent activity that is conducted against the financial institutions. I compiled some of this expertise in a 400 page book titled "Phishing Exposed", a technical manual discussing techniques to investigate and understand online fraud against financial institutions and other businesses. I was then invited by one of the co-authors of the FFIEC examination handbook to speak at the OCC on two-factor authentication, both on its strengths and its known weaknesses.

I have performed multiple types of risk analysis specific to fraud prevention for multiple financial institutions, including but not limited to Wells Fargo, TDWaterhouse, TDAmeritrade, Citigroup, Charles Schwab, Pay Pal, Ticketmaster, Wachovia, Chase and Washington Mutual. I have also been retained in the past to monitor several banks and trading companies for external

fraud activity including phishing attacks and malicious software threats. Pay Pal recently documented in an email that the defenses they use today are based on my existing research and suggested proposals, many from my book. I have spoken at APACS (known now as the UK Payment Association) in London providing expertise on the status of current online fraud techniques employed by cyber-criminals. Many banks in the UK attended and specifically pursued me to provide expert consulting including HSBC, RBC, RBS, and Barclays.

I have designed multiple technologies that assist in preventing and gaining intelligence against online fraud attacks. I have performed security protocol assessments, application security assessments and general security audits with the primary focus of determining the best action against external threats such as fraud, phishing, and malicious software (malware). I have analyzed anti-fraud software for TDAmeritrade specifically to determine if the technology was suitable against fraud in the long term.

I have designed advanced forensic technology that is actively distributed to law enforcement worldwide.

My expertise in online fraud has enabled me to travel the world to assist institutions and make many contributions to the banking community as well as law enforcement and the Department of Defense.

Lance James

lancej@gmail.com

WORK SUMMARY

Director of Intelligence, Vigilant, LLC, Present

Senior Threat Analyst, Damballa, 2010

CTO of Technology and Development, Secure Science Corporation, 2003-2010
Sample Projects: IntelliFound, penetration testing, architecture, forensics, malware analysis, cryptography

Technical Advisor, Numerous financial institutions, law enforcement and intelligence agencies, 2003-Present

Information Security Manager, Bakbone Software, 2001-2004
IT network security, risk analysis, application security, and applied cryptography

Principal Engineer & Software Development Manager, Invisiblenet, 2001-2003
Secure Distributed Computing, Intelligent Autonomous Systems, Applied Cryptography, Information Security

Independent Consultant, 1998-2001

KEY STRENGTHS

Strategic Technology Initiatives

- Founded InvisibleNet leading over 40 developers to design innovative technology
- Created the Mal-Aware network, encompassing over 1000 key members in the information security and anti-virus community
- Pioneered IntelliFound (Secure Science) Identity Surveillance enabling major financial institutions and governments real-time intelligence services necessary to fight e-crime and protect their customers
- Introduced many unknown vulnerabilities to the public enabling safe computing and telephony for the masses

Rapid Prototyping & Programming

- Developed secure memory management API for InvisibleNet
- Designed Security Template Software, a SAN/NAS cryptographic library (Secure Science)
- Designed ARE (Automated Reverse Engineering) for fast malicious software analysis in the field (Secure Science)
- Rapidly developed e-mail alert program for NetVault software under short notice (Bakbone Software)
- Developed many "on-the-fly" programs specifically designed for incident response and forensic cases (Secure Science)

Emerging Technology & Market Assessments

- First to publish forensic paper on the future problem of electronic crime known as phishing introducing high-profile clients to Secure Science
- Advised clients on purchases of emerging technologies based on sound analysis and marketing deployment techniques
- Analyzed emerging technologies detailing their realistic viability and life cycle in todays market

Team Building & Management

- Assembled 40 developers worldwide to successfully design, develop and maintain the open source project InvisibleNet
- Built and managed External Threat Assessment Team, Malicious Software Analysis Team, and engineering team at Secure Science Corporation solving problems successfully and designing innovative products and necessary tools

Strategic Corporate Planning

- Strategically positioned Secure Science as thought leader in electronic bank fraud, providing continuing successful business within a niche field
- Successfully foreseeing the needs of financial and government entities ahead of time, enabling adaptability and early strategic placement in specific favoring markets
- Establishing introduction of innovative "bleeding-edge" technology to standards bodies, organically embedding products and services within appropriate seasonal focus

Systems Integration & Administration

- Architect for WAN/LAN environment for Baker & McKenzie (independent consulting) utilizing Cisco Catalyst VLAN switches, and Cisco 7600 routers.
- Implemented Heterogenous environment featuring HP-UX, Solaris, AIX, FreeBSD and Windows NT for Xerox Corporation (independent consulting)
- Renovated WAN/LAN environment for Bakbone Software,encompassing secure traffic via IPSec for Video, Voice and Data communications.

Advanced Technology Research

- Invented pro-active (patent-pending) anti-fraud technology that report patterns that exist before initiated attacks
- IntelliFound – preemptive electronic discovery of compromised credentials & credit cards

Training, Development, & Mentoring

- Personally mentored interns at Secure Science enriching their advancements in education and career opportunities
- Involved in electronic crime and counter-intelligence training internationally for governments, universities, and corporations
- Published globally available educational books on electronic crime and emerging threats

Cross-Organization Collaboration

- Moderation of the Mal-Aware network consists of balancing financial institutions, government agencies, anti-virus researchers, Internet Service Providers and the information security community to effectively reach their goals.

Client Needs Analysis

- Established needs for a multitude of clients enabling a solid Statement of Work followed by excellent work product
- Identity Management client needs assessment conducted for one of the largest non-profit organizations
- Included in round table meetings with large clients as main advisor for client needs specifically in the subject of defense-in-depth analysis

Policy and Compliance Assessment

- Involved with handling SAS-70 audits within Secure Science as well as assistance for our clients.
- Interpretation of FFIEC two-factor guidelines provided to many financial institutions
- Assessment of Sarbanes-Oxley (SB1386) investigative reporting initiative conducted for clients
- Trainer for 21 CFR Part 11 for pharmacological company seminar
- Lectured on FFIEC, SOX, Title 18 USC 1030, and many other regulations worldwide
- Consistently aiding law enforcement involving interpretation of legal action in accordance with specific laws

Multiple Project Management

- Parallel management of External Threat Assessment Team, Malicious Software Analysis Team and engineering team
- Object oriented structure for engineering team, successfully requiring management of multiple aspects of a certain technology
- IntelliFound – managing a growing data center that houses over 7 terabytes of dynamic data, specifically designed for multi-usage real-time analysis.

SELECTED ACCOMPLISHMENTS

<u>Tasked development and creation of a worldwide fraud prevention and surveillance systems</u>

Responsibilities included:

Project Management
Incident Response/Mitigation
Inter-departmental Liaison
Cost-effective Strategy Implementation
New Technologies Deployment

Technical Advisor to numerous government agencies worldwide

Responsibilities include:

e-crime research and education
in-depth training/consulting
facilitating the collaboration between law enforcement and financial institutions*

*To date 67 arrests have resulted from partnerships

Author of Phishing Exposed, a reference guide utilized by universities, law enforcement and security researchers in a continuing effort to prevent on-line fraud attacks.

Founder of InvisibleNet, the first secure real-time anonymous peer-2-peer network.

Unveiled author of (name omitted) Virus through in-depth, targeted forensic analysis.

Charged with the deployment of a multi-national secure network, comprised of more than 1000 vetted individuals in the areas of law enforcement, intelligence, and e-crime research.

SELECTED PROFESSIONAL ACTIVITIES

Board Positions:

Digital PhishNet/NCFTA (A collaborative of Microsoft and the FBI Cyber-Crime Unit)
Toorcon (San Diego, InfoSec Conference)
Secure Science Corporation
InvisibleNet

Memberships:

San Diego 2600 Chapter
San Diego InfraGard Chapter
HTCIA Member San Diego Chapter
Arizona State University HoneyNet Project
Malicious Activity Awareness & Response
National Computer Forensics and Training Alliance
Anti-Phishing Working Group
Digital PhishNet

➢ **Highlighted Speaking Engagements:**

- Lecturer – Multiple Universities including RIT, UCSD, SDSU, and University of Wisconsin-Madison
- Expert Witness – House of Representatives (Bill HR5136)
- Keynote Speaker – Secret Service, Washington, DC (Electronic Crimes Task Force)
- Keynote – First Asia HTCIA Conference (Hong Kong)
- Panel Speaker – Central Intelligence Agency
- Panel Speaker – Anti-Spyware Coalition
- Keynote – Federal Bureau of Investigations
- Keynote – Digital PhishNet (Germany/San Diego)
- Keynote – SANS Conference (San Diego)

➢ **Training:**

- Trainer – Pentagon
- Trainer – First Asia HTCIA Conference (Hong Kong) – Malware Analysis
- Trainer – Central Intelligence Agency - Information Warfare
- Trainer – 21 CFR Part 11 (Deep Knowledge Seminars)
- Trainer – FFIEC two-factor initiative
- Trainer – Digital PhishNet (Germany)
- Trainer – SANS Conference (San Diego)
- Advisor – Secret Service, Washington, DC (Electronic Crimes Task Force)
- Advisor – Federal Bureau of Investigations

➢ **Notable Publications:**

- Author, "**Banking Scam Revealed**" - SecurityFocus Article
- Author, **Phishing Exposed** – Syngress Publishing
- Co-Author, **Emerging Threat Analysis**, - Syngress Publishing

---

RECOGNITION AWARDS

Federal Bureau of Investigation
1st Asia High Tech Crime Investigation Association
Central Intelligence Agency
Secret Service Electronic Crimes Task Force
Pentagon Computer Incident Response Team
Office of the Comptroller of the Currency
SANS

SELECTED TECHNOLOGY/POLICY KNOWLEDGE (at least 2-5 years cumulative experience)

Operating Systems: Linux, Windows 2000/XP/Vista/2003, Solaris, HP/UX, A/IX, UNIX, Macintosh

OS Add-ons: Terminal Services, Citrix MetaFrame, Citrix NFuse, SSH, X Window, Motif, AFS, Vmware

Languages: Perl, PHP, C, C++, JAVA, JavaScript, AJAX, Shell, x86 assembly

Databases: SQL, MySQL, PostgreSQL

WWW: HTML, XHTML, XML, CSS, DHTML, RDF, PICS, SSL, CGI, Unicode, Apache HTTP, ...

Messaging: Exchange, Postfix, Sendmail, Qmail. Asterisk (SendText) ...

Security/Network: firewalls, PKI, biometrics, routers and switches (Cisco/Nortel/HP/Dell/Juniper), Netscape (iPlanet) Proxy, digital signatures, encryption, RSA, content switches, VOIP (Cisco, Lucent, Asterisk, OpenSIP), VPN (Concentrators/FreeSwan/PiX/OpenBSD), smart cards, IDS Implementation and Signature Development - (Snort, Dragon, TippingPoint), DNS, wireless, Wi-Fi/802.11, SAN/NAS environments, Forensic software (Encase, Autopsy/Sleuthkit, FTK).

Governance Policy: CoBIT, FITSAF, FITSCAM, BS 7799-2, PCI, 21 CFR Part 11, Sarbanes-Oxley
Assessment Methodologies: ISECOM OSSTMM
Security Best Practices: ISO, SAS 70, NIST, GASSP, IETF, GAC, FFIEC
Compliance & ERP Software: AssureNet, ReconNet, STS, JD Edwards, Documentum Compliance Manager

Antiquated: Gopher, LISP, Ultrix, VMS, Sun/OS, Pascal, BASIC, Z80 Assembly

Applied Concepts: distributed computing, information life-cycle management, storage networks, software development life-cycle, reverse engineering, language identification, computational linguistics, information retrieval, thin-client computing, electronic fraud countermeasures, caller-id spoofing, multicasting, unicasting, credit-card processing, rapid prototyping, human-computer interface, usability, computer-support collaborative work, content management, disciplined programming, digital libraries, artificial intelligence, mobile code and agents, e-commerce, information organization/taxonomy, knowledge engineering, cryptography, computer and Internet forensics, load-balancing, fault-tolerance, visualization, virtual machine environments

---
