IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

MICROSOFT CORPORATION, a Washington corporation, FS-ISAC, INC., a Delaware Corporation, HEALTH-ISAC, INC., a Florida corporation, Plaintiffs, v. DENIS MALIKOV, and JOHN DOES 1-7, Defendants.	)	Civil Action No: **FILED UNDER SEAL**

DECLARATION OF ERROL WEISS IN SUPPORT OF PLAINTIFFS' APPLICATION FOR AN EMERGENCY *EX PARTE* TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION

I, Errol Weiss, declare as follows:

I. Declaration

1. I am the Chief Security Officer of the Health Information Sharing & Analysis Center (Health-ISAC). I make this declaration in support of Plaintiffs' Application for an Emergency Temporary Restraining Order and Order to Show Cause re Preliminary Injunction. I make this declaration of my own personal knowledge or on information and belief where noted. If called as a witness, I could and would testify to the truth of the matters set forth herein.

II. Introduction

2. I am employed by Health Information Sharing & Analysis Center (Health-ISAC) since April 2019. In my role at Health-ISAC, I created and staffed Health-ISAC's Threat Operations Center in Titusville, Florida, providing over 700 global health organizations with meaningful and actionable threat intelligence relevant for information technology and information security professionals in the healthcare sector.

3. I work with Microsoft to disrupt criminal malware and botnets responsible for significant fraud losses impacting financial institutions and their customers, resulting in three subsequent civil actions including successful disruptions of Zeus (2012), Citadel (2013) and Shylock (2014).

4. I have over 25 years of experience in Information Security. Prior to joining Health-ISAC, I was the Senior Vice President at Bank of America (2016-2019), overseeing the Global Information Security and Cyber Threat Intelligence teams. I worked with internal partners to protect information, customers and staff by reducing the impact from cyber threats. From 2006 to 2016, I led Citigroup's Cyber Intelligence Center, a global organization that provides actionable intelligence to thousands of end-users across the entire enterprise. In 2012, I testified as an expert witness before the House Financial Services Committee's Subcommittee on Capital Markets and Government Sponsored Enterprises at the "Cyber Threats to Capital

Markets and Corporate Accounts" hearing.

5. I began my career with the National Security Agency (NSA) conducting vulnerability analyses and penetrations of highly classified U.S. Government systems and then spent ten years with consulting firms delivering information security services such as managed security services, security product implementations and secure network designs for Fortune 100 companies. A current version of my curriculum vitae is attached to this declaration as **Exhibit 1.**

A. <u>Overview of Ryuk</u>

6. My declaration concerns a ransomware referred to as "Ryuk." Ransomware is a form of malicious software (malware) designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption.

7. Ryuk has been linked to more than 200 ransomware attacks impacting hospitals, public health departments, nursing homes and patient care facilities around the world since 2018. The attacks resulted in the temporary or permanent loss of IT systems that support many of the provider delivery functions in modern hospitals resulting in cancelled surgeries and delayed medical care. The Defendants in this case have directed such malware over the Internet to many victim computing devices through the ZLoader botnet. A "botnet" is a network of computing devices comprised of Internet-connected computing devices that have been infected with

some form of malware.

8. Specific examples of impacts caused by Ryuk at patient care facilities in the United States since 2018 include:

i. Ryuk attack forced ambulances to divert, causing a 90-minute delay in emergency patient services;
ii. Ryuk disrupted delivery of chemotherapy treatments for cancer patients;
iii. Ryuk forced hospitals to cancel elective procedures;
iv. Ryuk caused delays in reporting of laboratory results;
v. Ryuk caused delays in scheduling appointments for maternity and oncology patients;
vi. Ryuk caused more than three weeks of downtime for the Electronic Health Records management system;
vii. Ryuk impacted systems at nursing homes, causing patient records to be unavailable and pharmaceuticals orders could not be placed; and
viii. Ryuk leaked sensitive patient data including treatments, diagnoses, and other information of hundreds of thousands of people.

B. <u>Threat Intelligence Related to Ryuk</u>

9. Hospitals reported revenue losses due to Ryuk infections of nearly $100 million from data I obtained through interviews with hospital staff, public statements, and media articles. The Ryuk attacks also caused an estimated $500 million in costs to respond to the attacks – costs that include ransomware payments, digital forensic services, security improvements and upgrading impacted systems plus other expenses.

10. The Ryuk ransomware attacks impacted hundreds of health care

facilities across the U.S. Victims include hospitals and patient care facilities located in more than 192 cities in 41 states and the District of Columbia. To provide additional detail for the benefit of the court, Ryuk victims were located in several Georgia cities including Atlanta, Augusta, Dunwoody, Sautee and Savannah. **Chart 1** below provides an overview of the number of cities impacted by Ryuk:

State	# Cities	State	# Cities
AK	2	MS	5
AL	2	NC	3
AR	3	ND	1
AZ	2	NJ	2
CA	10	NM	2
CO	2	NV	5
CT	1	NY	5
DC	1	OH	5
DE	2	OK	3
FL	18	OR	2
GA	9	PA	10
IA	1	SC	5
ID	2	TN	7
IL	5	TX	24
IN	6	UT	6
KY	4	VA	10
LA	2	VT	3
MA	4	WA	3
MI	7	WI	2
MN	1	WV	1
MO	3	WY	1

Chart 1.

11. The Defendants deployed Ryuk through ZLoader and disseminated the ransomware to victim computers.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct to the best of my knowledge. Executed this 3rd day of April, 2022, in Jacksonville, FL.

Errol Weiss

EXHIBIT 1

Errol S. Weiss

+1 321-209-9898 Email: eweiss@h-isac.org

Summary

Accomplished information security executive recognized internationally in the healthcare and financial services sectors as a visionary and a leader in threat intelligence operations and management. Proven ability to build information security strategies aligned to business risk and corporate goals.

PROFESSIONAL EXPERIENCE

Health Information Sharing & Analysis Center (H-ISAC) **April 2019 to Present**
Chief Security Officer, Titusville, FL

Responsible for the strategic vision and direction of H-ISAC's day-to-day Cyber and Physical Security Services offered to H-ISAC member organizations. Managing the delivery of Cyber and Physical Threat Intelligence and oversight of the H-ISAC Security Operations Center (SOC) functions and staff. Providing direction and leadership for identity services, community exercises and other special interest services for the H-ISAC membership.

Bank of America, Global Information Security, Senior Vice President **May 2016 to April 2019**

5/2016 – 10/2017: **Director, Cyber Threat Intelligence**, Developed the strategy and vision to create a world-class cyber threat intelligence function. Established a new organizational structure to support the intelligence management lifecycle (requirements, collection, analysis, dissemination and feedback) and recruited diverse top talent into key leadership positions. Created new services and intelligence products, increased outreach and internal partnerships, established 24x7 follow-the-sun analyst coverage, rolled out a new mobile app intelligence monitoring service and began implementing a responsible vulnerability disclosure program. Enhanced the collaboration and partnerships between the firm and public sector entities including US Treasury, US Secret Service, DHS and FBI.

11/2017 – 4/2019: **Business Process Cyber Assessments Executive**, Responsible for end-to-end assessments of critical applications across the Bank of America enterprise. Leading business process assessments of critical systems focusing on cyber risks from people, processes, technology and third parties. Manage teams of assessors conducting reviews on an on-going basis.

Citi **September 2006 to April 2016**
Cyber Intelligence Center Director, New York, NY

Identified the need and obtained senior management support to create an intelligence collection and analysis center. Successfully built and grew a world-class Cyber Intelligence Center focused on providing actionable intelligence of threats against the financial services sector and those specifically targeting Citi employees, assets, business operations and technology infrastructure worldwide. Established intelligence management processes, implementing them in an on-line platform supported by analysts in strategic global locations to support a 24x7 follow-the-sun model. Formulated interaction models with key parts of Citi including fraud risk management, incident management, information security, threat management, physical security, investigations and business operations. Accountable for organizational plans and managing a staff of 40 in seven global locations. Provided mentoring, completed performance reviews, managed budgets and influenced change to global policies and procedures. Reported directly to Citi's Chief Information Security Officer and Global Head of Information Security. Presented at several FS-ISAC Conferences and met with peer financial institutions to share concepts about the intelligence management functions and helped others build their own intelligence capabilities.

Member of Citi's Information Security Risk Operating Committee, responsible for setting enterprise information security policy, reviewing operational metrics and performance and interaction with regulators globally including the Federal Reserve Board and the Office of the Comptroller of the Currency (OCC) in the US and the Monetary Authority of Singapore in Asia.

Interacted regularly and promoted information sharing and cyber security with top level management at other financial institutions, US Congressional Leaders and their staff, US Government organizations, US Intelligence Community, senior officials and regulators from foreign governments, and third-party providers. Partnered with private banking and institutional investment staff to present regularly to high net worth individuals and commercial institutions about staying safe on-line and providing simple advice to them stay secure on-line.

SAIC **February 2004 to September 2006**
Assistant Vice President, Managing Director, Reston, VA
Division manager for 20 staff including two operations managers and a chief scientist. Responsible for daily operations and customer relationships for the Information Sharing and Analysis Center (ISAC) and Open Source Monitoring (OSM) services. Provided cyber and physical vulnerability, threat and incident information to more than 1,800 financial institutions predominantly in the United States and customized consultative threat intelligence to large international corporations.

Responsible for personnel management, profit and loss management, financial planning, new sales, service delivery and service quality. Held frequent interactions with customers, including the FS-ISAC Executive Director and the Board of Directors. Actively participated in monthly board meetings, bi-annual membership meetings and membership campaigns. Improved service quality through feature enhancements, partnerships and oversight of operations.

Led the selection and transition teams responsible for migrating ISAC operations to another service provider. Worked closely with the new management and operations teams to ensure a smooth, seamless transition and complete customer satisfaction.

Solutionary, Inc. **August 2002 to January 2004**
Vice President of Technical Services, McLean, VA
Managed the professional services organization for a security services provider based in Omaha, Nebraska. Areas of responsibility included oversight of project management, information security services delivery and sales engineering for services such as Risk Assessments, Visa CISP Certifications, Secure Network Designs, Security Product Implementations, Managed Security Services, Incident Response and Penetration Testing. Provided senior technical leadership and consulting support for information protection and assurance programs to clients in the finance, banking and insurance areas. Responsible for business development with key named accounts.

Predictive Systems, Global Integrity and SAIC (Northern Virginia) **May 1996 to July 2002**
Global Integrity was a wholly owned SAIC subsidiary. Predictive Systems acquired Global Integrity in 2000.

12/2000 – 7/2002: **Vice President Services Strategy.** CTO of managed services unit responsible for product management and services strategy including managed firewall, managed intrusion detection, information sharing, Open Source Intelligence, managed vulnerability assessments, and Incident Response / Digital Forensic services. Collaborated with engineering, operations, business development and sales organizations to establish a suite of packaged services that could be implemented and delivered with high value. Responsible for establishing and maintaining relationships with security product vendors and resellers strategic to future growth plans.

8/1998 – 12/2000: **Vice President and Division Manager**, Managed Security Services. Created the vision and implemented a new Security Operations Center to provide remote monitoring and management of firewalls and intrusion detection systems. Recruited staff and provided key leadership. Performed business development operations support for the entire operation and achieved more than $2 Million in revenue. Established several key reseller and channel marketing opportunities. Recognized by management team as a key individual contributing to the success of Global Integrity.

5/1996 – 8/1998: **Division Manager**, Information Protection Operations, Responsible for division management of a $4.6 million business and for the supervision of over 30 employees. The division had four major information security programs, including computer and network vulnerability assessments for Fortune-100 clients.

Computer Sciences Corporation (CSC) **November 1995 to May 1996**
Senior Member Advisory Staff, Hanover, MD
Directed computer and network penetration efforts for US Government and commercial customers. Task area leader for INFOSEC Technical Services. Conducted marketing activities, wrote white papers, formulated a vulnerability assessment methodology. Lead author on several commercial INFOSEC proposals that resulted in $1 million in new business.

National Security Agency (NSA) **August 1987 to November 1995,**

12/1993 - 11/1995: **Senior Network Security Analyst**. Technical team leader on network security analysis and evaluation projects for the Systems and Network Attack Center. Provided technical guidance to evaluation team analysts and to end-users. Performed network vulnerability assessments and penetration testing on classified US Government networks and assessed the ability of insiders and outsiders to penetrate network systems. Conducted research on vulnerabilities of operating systems, hardware platforms, software applications and network protocols. Authored detailed technical reports on system vulnerabilities and appropriate countermeasures and provided INFOSEC engineering support to end-users.

8/1987 - 12/1993: **Computer Engineer and System Development Manager**. Provided system level developmental support for a major intelligence production system. Studied secure computing architectures and coordinated strategic plans for the transition of operational systems to implement a secure computing infrastructure. Developed system security requirements and specifications for an advanced intelligence processing system.

AFFILIATIONS and PROFESSIONAL MEMBERSHIPS

Singapore Healthcare Cybersecurity Advisory Panel **October 2019 to Present**
Appointed by Singapore's Ministry of Health to represent the Health-ISAC and U.S. perspectives on the evolving threat landcape, best practices and current and future cybersecurity initiatves for Singapore's healthcare sector.

Board of Directors, Financial Services ISAC **March 2010 to April 2016**
Board of Directors, Financial Services Information Sharing & Analysis Center (FS-ISAC). Non-profit organization owned and operated by the banking and finance sector and led by a Board of Directors of senior executives and security professionals from the world's top financial institutions. Delivered strategic direction for mission and purpose, ensured effective organizational planning, provided resources for key activities, determined and monitored programs / services offered to the membership and enhanced the organization's public image. Served as Vice-Chairman, Board of Directors (2016).

Key accomplishments include:

- Following a sharp rise in fraud, created the Account Takeover Task Force in 2010 and led it for two years. The task force was made up of over 120 individuals from thirty- five financial services firms, ten industry associations and processors and representatives from seven government agencies. The task force developed best practices focused on prevention, detection and responsiveness to ensure an improved and effective defense against cyber crimes, including account takeover. The task force created surveys and collected actual fraud loss figures from hundreds of financial institutions to create a baseline that could later be used to demonstrate the effectiveness of industry efforts (like this task force) to reduce fraud.
- In 2012, championed the partnership between FS-ISAC and Microsoft to work together on disrupting criminal malware and botnets responsible for significant fraud losses impacting financial institutions and their customers. Personally led the finance sector efforts and coordination of legal,

technical and public relation strategies for three subsequent civil actions including Zeus (2012), Citadel (2013) and Shylock (2014).

FCC CSRIC Appointed Member **May 2013 to May 2015**
Appointed member to represent the financial services sector on the Federal Communications Commission (FCC) Communications, Security, Reliability and Interoperability Council (CSRIC).

Advisor to Board of Directors, Financial Services ISAC **February 2006 to March 2010**
Appointed as Advisor to Board of Directors, Financial Services Information Sharing & Analysis Center (FS-ISAC). Provided guidance on business processes, operational improvements and marketing support to the Board of Directors.

EDUCATION

Johns Hopkins University, MS, Technical Management with a focus in Organization Management
Bucknell University, BS Engineering, Computer Engineering with a minor in American Literature

PATENTS

Co-Inventor (patent 6,807,569, issued October 19, 2004) for "Trusted and anonymous system and method for sharing threat data to industry assets"

PUBLICATIONS

Network Forensics & Analysis Tools, **cover story** for Information Security Magazine, February 2002.

A Case Study: Penetration Testing, National Computer Security Center / National Institute of Standards and Technology Conference Proceedings, October 1996.
http://csrc.nist.gov/nissc/1996/papers/NISSC96/paper045/nissc.pdf

EXPERT TESTIMONY

June 1, 2012, testified before the House Financial Services Committee's Subcommittee on Capital Markets and Government Sponsored Enterprises at the "Cyber Threats to Capital Markets and Corporate Accounts" hearing. http://financialservices.house.gov/Calendar/EventSingle.aspx?EventID=296813
Video Archive: https://www.c-span.org/video/?306361-1/cyberthreats-us-financial-industry

SECURITY CLEARANCES

2009 – Present: Active TS-SCI through U.S. Department of Homeland Security's Private Sector Clearance Program