Exhibit 1

Maurice Eduardo Mason

Phone: [redacted]
E-mail: [redacted]
Clearance: Active Top-Secret (TS)

SUMMARY OF QUALIFICATIONS

- Experienced investigator specializing in computer investigations. Trained and experienced in hacker methodology/techniques, computer forensics, incident response, electronic discovery, blockchain analysis, litigation support and network intrusion investigations.
- Proficient in utilizing a variety of commercial and open-source tools (e.g. Magnet Axiom, Autopsy, Volatility, EnCase, FTK, RemNux, Zimmerman Tools, MDE, Carbon Black, Flare etc..) to guide an investigation.
- Real-world experience responding to Advanced Persistence Threats (APT) and ransomware attacks from both public and private sectors. This includes familiarity with Indicators of Compromise (IOCs), Indicators of Activity (IOAs) and Attack Tools, Techniques and Procedures (TTPs).
- Proficient in leading incident response engagements to guide clients through forensic investigations, contain security incidents, and provide guidance on longer-term remediation recommendations. Motivated to see the big picture, understanding evolving attacker behavior and intent.
- Proficient in Query languages such as Kusto Query Language (KQL) to conduct threat hunting and or forensic analysis at a large scale.
- Experience with analyzing a wide variety of logs and telemetry including AV, web server, SIEM (Azure Sentinel), Unified Audit Log (UAL), Entra AD Sign/Audit etc.)
- Possess a working knowledge of malware analysis (static/dynamic) such as unpacking, deobfuscation and anti-debugging techniques when analyzing malicious code.
- Experienced with working and or collaborating with SOC and CSIRT service teams.
- Strong client facing background in both supporting Federal Government and Private Sector clients.
- 8+ years' experience working within the Information Technology and Cyber Security departments.

EMPLOYMENT HISTORY

Microsoft **February 2023– Present**
Senior Investigator

- Senior Investigator on the Microsoft Digital Crimes Unit (DCU) focusing on Ransomware.
- Conduct proactive ransomware investigations to identify critical command control infrastructure, ransomware payments and ransomware actors to develop disruption strategy to eliminate or severely cripple cyber-criminal ecosystem.
- Build cases against prolific Ransomware actors/groups collaborating with the Microsoft Threat Intelligence (MSTIC) team, resulting in highly impactful criminal referrals yearly.
- Work with public (law enforcement, country certs) and private sectors, and develop international partnerships to support ransomware disruptions on a global scale.
- Document and identify monetization schemes utilized by cyber-criminals ranging from online advertising fraud, ransomware, and targeted financial fraud.
- Cluster and model data related to ransomware to help identify, document and monitor tactics, techniques and procedures used by threat actors related to ransomware groups.
- Collaborate with Microsoft legal and Microsoft Threat Intelligence (MSTIC) teams to develop new strategies to disrupt cybercrime through both civil and criminal proceedings.

Microsoft **August 2021– February 2023**
Senior Digital Forensics Consultant

- Lead forensic analyst on Microsoft's Detection and Response Team (DART), conducted proactive and post reactive incident response investigations for large-scale clients with complex networks impacted by various security incidents.
- Investigated data breaches (Ransomware, Network Intrusions, Unauthorized Access, APT, Vulnerabilities) by leveraging forensics tools and EDR/SIEM solutions to determine the root cause analysis (RCA) of compromises and malicious activity that occurred in client environments.
- Analyzed host, network, memory, cloud and other available data sources to define the scope of an incident, develop a timeline of threat actor activity, and inventory data populations likely accessed/exfiltrated based on forensic artifacts.
- Conducted security assessments (host and cloud) to identify areas of risk and provide specific technical guidance to help ensure any gaps are remediated within clients environment.
- Built and presented PowerPoint outbriefs for both technical and executive audiences when detailing analysis related to root cause analysis, persistence mechanisms, lateral movement and the full extent of the compromise while prioritizing the next steps for remediation.
- Contributed to the development of runbooks for forensic analysts to follow, playbooks were mapped to MITRE ATT&CK Framework to improve processes and information sharing across teams.
- Interviewed new candidates as well as trained/mentored new hires that were staffed.

TracePoint LLC **June 2020– June 2021**
Senior Digital Forensics Consultant

- Conducted proactive and post reactive incident response investigations on small and medium size organizations included but were not limited to host-based analysis, memory analysis and network analysis through investigating Windows and Cloud data sets to identify Indicators of Compromise (IOCs) for clients who have reported cyber incidents.
- Investigated data breaches (Ransomware, Network Intrusions, Unauthorized Access) leveraging forensics tools and EDR/SIEM solutions to determine the root cause analysis (RCA) of compromises and malicious activity that occurred in client environments.
- Lead multiple engagements in guiding clients through forensic investigations, including but not limited to triage, root cause analysis, escalations, malware analysis and determining severity level of incidents.
- Produced comprehensive and accurate reports for both technical and executive audiences when detailing analysis to clients detailing root cause analysis, remediation steps and preventative measures.
- Led development of a new reporting template which included executive summary as well as full forensic report to drive reporting consistency across all analyst reports.

ManTech International **June 2019– June 2020**
Senior Computer Forensic Analyst

- Contracted to Department Justice (Executive Office of US attorneys Division) to conduct cyber forensic investigations and analysis.
- Act as the most senior forensic analyst on a team of three, helped revamp the Forensics/eDiscovery program from the ground up, making it an operational program within 4 months from ideation to production. Introduced new policies/procedures and tools.
- Created a formalized triage methodology for forensic artifacts, as well as implemented a malware analysis laboratory utilizing virtual machines for malware analysis/research.
- Conducted host-based analysis for Indicators of Compromise (IOCs) detected by Security Operations Center (SOC) to help determine root cause and deter malware presence. Mapped IOCs to MITRE Attack Framework to be used as use-cases.
- Produced comprehensive and accurate reports for both technical and executive audiences when detailing analysis to clients.

BlackBag Technologies **April 2018– June 2019**
Computer Forensic Analyst

- Contracted to the Department of Defense Cyber Crime Center DC3/DCFL, conducted forensics acquisition and analysis in support of criminal investigations (Child exploitation, Sex offense, Fraud, Narcotics, Homicide, Drug/Human Trafficking).
- Provide detailed documentation on In-depth analysis related to file system analysis, mobile forensic analysis, registry analysis and internet history analysis.

Innovative Discovery LLC **April 2015 – April 2018**
Digital Forensic Consultant

- Serving as a client facing Forensic Consultant for an E-Discovery litigation company.
- Performed forensic data acquisition of desktops, laptops, hard drives, servers, cell phones, external media, emails and various other types of data sources.
- Conducted forensic analysis involving intellectual property, financial, employee misconduct, and fraud.

LS Technologies **June 2013-April 2015**
System Analyst

- Contracted to the Federal Aviation Administration C3 department, oversaw integration of user workstations with Microsoft Windows server OS and Active Directory.
- Responded to multi-channel support requests (Helpdesk) from employees and customers seeking help with software or computer related issues.

Educational Background:

Champlain College, Burlington, VT
Master of Science - Digital Forensics Graduated: August 2017

Bowie State University, Bowie, MD
Bachelor of Science - Computer Technology Graduated: December 2014

Professional Certifications:

- EC-Council Computer Hacking Forensic Investigator (CHFI) May 2018
- Department of Defense Digital Forensic Examiner October 2018
- Department of Defense Digital Media Collector October 2018
- EC-Council Certified Ethical Hacker (CEH) December 2018
- GIAC Smartphone Forensics Analysis In-Depth (GASF) August 2019
- GIAC Certified Forensics Examiner (GCFE) September 2019
- GIAC Certified Incident Handler (GCIH) November 2019
- GIAC Certified Forensic Analyst (GCFA) December 2020
- GIAC Certified Defender (GDAT) February 2022
- TRM Certified Investigator (TRM-CI) April 2023
- Chainalysis Reactor Certification (CRC) April 2023
- Investigation Windows Endpoints (Gold) April 2023
- GIAC Cyber Threat Intelligence (GCTI) June 2023