Exhibit 1

Christopher Stangl
BERKELEY RESEARCH GROUP, LLC
[redacted]

Direct: [redacted]
[redacted]

SUMMARY

Christopher Stangl is a managing director in BRG's Cybersecurity and Investigations practice. A veteran FBI Agent, he spent his law enforcement career investigating cybercrime, shaping national cyber policy, and working directly with private industry through the Federal Bureau of Investigation's public/private partnerships. His tenure in government encompassed the full range of cyber threats facing corporations and individuals, from ransomware to advanced persistent threats.

Mr. Stangl leverages his deep cybersecurity expertise to help clients tackle and overcome a wide range of data security, data protection, and privacy challenges. He specializes in the design and implementation of robust cybersecurity programs to safeguard critical assets, proactive threat intelligence, complex cyber investigations, and navigating the legal and regulatory implications of security incidents.

Before joining BRG, Mr. Stangl had a distinguished career spanning over twenty years as an FBI Special Agent, including as a member of the FBI's Senior Executive Service. He most recently spearheaded the implementation of a cybersecurity program within the FBI's Science and Technology Branch, safeguarding critical resources across multiple divisions. Mr. Stangl adhered to industry standards and best practices, including the NIST Cybersecurity and Risk Management Frameworks.

Mr. Stangl investigated a wide range of cyber cases at the FBI, including computer intrusions by cybercriminals and nation-states, counterintelligence and insider threats, intellectual property rights violations, online child exploitation, extortion, and internet fraud. The cases for which Mr. Stangl was responsible included matters involving millions of dollars of illicit funds transferred to Russia via a digital currency exchange; a cross-jurisdictional, coordinated takedown of over seventy cybercriminals associated with the "Zeus Trojan" email malware; the apprehension and conviction of the creator of "Gozi" malware; a multinational investigation into the use of stolen account information from a hacked ATM network, resulting in nine convictions and millions of dollars seized in cash and property; dismantlement of the LulzSec hacking group; and the FBI's response to nation-state–sponsored distributed denial-of-service (DDoS) attacks on US banks' websites—the most significant and sustained DDoS attacks against US critical infrastructure originating from a nation-state actor in history.

Mr. Stangl held leadership roles at the FBI's New York and Newark field offices as well as FBI headquarters in Washington, DC. He served as Assistant Special Agent-in-Charge at the FBI Newark field office, leading the Joint Terrorism Task Force, Counterintelligence squads, and Cyber Task Force. He also was Chief of Operations for the National Cyber Investigative Joint Task Force, enhancing interagency information exchange and intelligence integration in the cyber field.

Mr. Stangl earned a number of awards for distinguished government service, including the FBI Director's Award for Excellence in Outstanding Cyber Investigation in 2010 for his instrumental role in identifying and

dismantling an international cybercrime organization that targeted US critical infrastructure; and again in 2011 for his leadership in an innovative investigation into a prolific cybercrime enterprise.

During his time at the FBI, Mr. Stangl emphasized partnering with the private sector by fostering shared situational awareness of the cyber threat landscape through collaboration, information exchange, and intelligence sharing. In 2015, he received the Director of National Intelligence's National Intelligence Community Award for Intelligence Integration for leadership in neutralizing a threat country through analytic, operational, and outreach initiatives.

Work History

Section Chief, Senior Executive Service (SES), Federal Bureau of Investigation, 06/2020 to 06/2023.
FBI – Washington, DC

Science and Technology Branch (STB)

- Architected and led the implementation of a cybersecurity program to protect high-level scientific and operational technology resources used for investigations and intelligence across the Criminal Justice Information Services, Laboratory, and Operational Technology Divisions, using industry standards and best practices such as the NIST Cybersecurity and Risk Management Framework (NIST SP 800-37).
- As a senior advisor and SME to the Executive Assistant Director, worked with FBI executives to identify, monitor, and reduce risk in conjunction with the FBI Office of the Chief Information Officer (OCIO).
- Created a unique risk register to provide executives with empirical data and expert opinion to make risk-based decisions.
- implemented a cybersecurity sprint plan with a catalog of security and privacy controls (NIST SP 800-53) to protect organizational operations and assets from a variety of threats.
- To increase awareness and improve the culture, educated stakeholders on cybersecurity, including developing a Cybersecurity Principle statement for STB and ensuring its adoption.

Cyber Division

- Executive-led the National Cyber Investigative Joint Task Force (NCIJTF), a multi-agency national focal point comprised of more than 30 law enforcement, intelligence, and Department of Defense agencies with co-located representatives working together to fulfill the U.S. Government's mission. Utilized technology to widen the scope of interagency communication and integration of intelligence.
- Responsible for leading the FBI Cyber Division's 24/7 Federal Cyber Center, Cyber Watch, to ensure the FBI complied with the Presidential Policy Directive (PPD-41) and U.S. Cyber Incident Coordination. In charge of coordinating notable activities in response to cyber threats:
    - **Log4J:** Exploitation of critical remote code execution (RCE) vulnerabilities in Apache's Log4j software library, including CVE-2021-44228 (known as "Log4Shell"), CVE-2021-45046, and CVE-2021-45105.
    - **SolarWinds Response:** Supply-chain attack of SolarWinds Corporation by the Russian Foreign Intelligence Service.
    - **Kaseya VSA Supply-Chain Ransomware Attack:** Supply-chain ransomware attack exploiting a vulnerability in Kaseya VSA software against multiple managed service providers (MSPs).

- **Colonial Pipeline Networks Ransomware Attack:** Ransomware attack on Colonial Pipeline Company networks, impacting the oil supply along the East Coast.

Assistant Special Agent-In-Charge (ASAC), 01/2017 to 06/2020
FBI – Newark, NJ

- Responsible for leading National Security programs, including the New Jersey-based Joint Terrorism Task Force (JTTF). This JTTF was comprised of investigators and analysts from various law enforcement and intelligence agencies, and its primary duties included conducting counterterrorism investigations, collecting and sharing intelligence for shared situational awareness, responding to threats and incidents, and crisis management. Additionally, led the Counterintelligence program to prevent and investigate intelligence activities in the U.S., as well as the Cyber program to investigate cyber attacks and provide subject matter expertise to the private sector in support of network defense efforts.
- Partnered with the New Jersey Office of Homeland Security and Preparedness to create the Biotechnology Threat Focus Cell (BTFC) to recognize and reduce threats to the biotechnology industry that are related to national security and insider threats. Encouraged threat sharing with private sector companies, which improved cooperation, intelligence and pattern sharing, and tackled issues that the industry is dealing with. Fostered intelligence sharing during Operation Warp Speed, a federal effort that expedited the growth of numerous COVID-19 vaccine candidates.

Acting Section Chief, Cyber Division, 06/2014 to 12/2016
FBI – Washington, DC

- Established a new cybercriminal operations section to provide oversight and assistance to field operations, allowing them to disrupt cyber adversaries, as well as analyze and provide intelligence for operational action and the protection of victims.
- Oversaw executive operations of three locations, including the Cyber Initiative and Resources Fusion Unit, Internet Crime Complaint Center, and Major Cyber Crimes Unit. Created initiatives to disrupt the cybercrime ecosystem in terms of malware, infrastructure, communications, and financial. Maintained contact with management, co-workers, external agencies, government officials, media, and the public. Drove the workforce to reach goals through respect, mentorship, and guidance. Set a vision and created plans to attain goals and objectives. Made decisions after examining all related circumstances, events, and options.
- Formed an international cybercrime coordination cell to unite the FBI's most important international and domestic partners in the battle against cybercrime in one place. A cross-functional multi-national development team was set up to design a standardized database schema to normalize various data types, such as bulletin boards, private messages, image galleries, blogs, marketplaces, and virtual currency databases, to enhance information sharing and reduce the time needed to identify actors and link criminal activity.

Unit Chief, Cyber Division, 07/2012 to 05/2014
FBI – Washington, DC

- Headed a team to identify and defeat nation-state adversaries that were targeting U.S. critical infrastructure from the Middle East and Africa. Implemented a model for private sector coordination which involved the rapid

distribution of reliable indicators; classified briefings to provide more information; and cooperation among competitors to promote the exchange of best practices to support collective defense.
- Created the FBI Liaison Alert System (FLASH) report to supply important technical data compiled by the FBI to private sector partners, aiming to equip recipients with effective intelligence to assist in the quick reaction in combating threats.

Supervisory Special Agent, 01/2010 to 06/2012
FBI – New York, NY
- Led a team investigating complex cybercrime matters on behalf of the FBI with a direct impact on the welfare, economy, and security of the United States.
- Collaborated with the United States Attorney's Office, local, state, and federal partners, Legal Attaché Offices, the FBI's overseas offices, and foreign law enforcement counterparts to create strategic partnerships, plans, and initiatives that aided in apprehending and prosecuting international cyber criminals.

Special Agent (Cyber), 05/2003 to 12/2010
FBI – Oklahoma City, OK
- Duties included investigating cybercrime related to computer intrusions, intellectual property rights violations, online child exploitation, extortion, and Internet fraud.
- Member of the FBI's Cyber Action Team (CAT), a rapid-response team that could be deployed anywhere in the country to handle major cyber incidents.
- Program coordinator for the Oklahoma chapter of the InfraGard Members Alliance, a joint venture between the FBI and the private sector to safeguard U.S. Critical Infrastructure.

Notable Milestones

Loomis, Fargo, and Company High Tech Heist
I successfully investigated an operations manager who had unlawfully obtained an encrypted combination for a bank drop box in an Oklahoma City, Oklahoma mall and stole more than $200,000 over a Thanksgiving weekend. This resulted in one of the earliest jury trial convictions of the Computer Fraud and Abuse Act (CFAA) in the State of Oklahoma.

Operation Cardshop
I conceived and led an undercover operation targeting online criminals engaged in the theft and trafficking of stolen financial and personal identification data, known as "carding." This operation established an undercover forum, called "Carder Profit," which allowed users to discuss criminal activity, make offers to sell and exchange goods and services related to carding, among other things. The purpose of the operation was to identify cybercriminals, investigate their crimes, and protect innocent victims from harm. The FBI was able to monitor discussion threads posted to the site, as well as private messages sent between registered users, and record the Internet Protocol addresses of users' computers when they accessed the site. Coordinated action by 34 FBI offices and 20 foreign law enforcement partners across 15 countries resulted in over 120 enforcement actions, including 27 arrests, 30 subject interviews, 30 search warrants, and the prevention of over $205 million in economic losses, protection of over 400,000 potential

cybercrime victims, and the notification of over 40 companies, government entities, and educational institutions of the breach of their networks.

Iran DDoS Attacks Private Sector Coordination

I led the FBI's response to Iran state-sponsored Distributed Denial of Service (DDoS) attacks conducted by Islamic Revolutionary Guard Corps-Affiliated Entities on U.S. banks' websites, which were the most significant and sustained DDoS attacks against U.S. critical infrastructure originating from a nation-state actor in history. To help the targeted victims, I created the FBI Liaison Alert System (FLASH) report, which provided attack indicators and was key for private industry as the FBI was able to articulate that the indicators were of "high confidence," meaning companies knew the actions they took would not affect legitimate customers. Disseminated 35 FLASH messages having over 115,000 attack indicators and supplied classified threat briefings to Chief Information Security Officers (CISOs) from 145 financial institutions and government agencies. Through this outreach and expedited release of indicators, the FBI was able to reduce the impact of DDoS attacks and established a best practice for the dissemination of information related to other cyber threats.

Saudi ARAMCO Investigation

I assembled a team and traveled to the Kingdom of Saudi Arabia (KSA) to investigate a major cyberattack on ARAMCO, an oil company, which rendered over 30,000 desktop computers inoperable. With the support of KSA, my team studied the available intelligence and evidence to create a one-page overview of the attack and a whitepaper containing details such as malware executables, files, MD5 hashes, and registry keys. This information was used to give threat briefings to oil and gas companies, as well as to bolster the defense of critical infrastructure.

Lulzec Hacktivist Group Investigation

I led a team in the investigation of the Lulzec hacktivist group, which had orchestrated hundreds of cyber-attacks that compromised the security of government, education, financial services, entertainment, and technology entities. Through collaboration with our partners, my team successfully identified, apprehended, and gained the cooperation of the group's leader, Hector Monsegur, also known as "Sabu". The pinnacle of our investigation was the arrest of Jeffrey Hammond, also known as "Anarchaos", who was responsible for high-profile intrusions such as the Strategic Forecasting, Inc. hack, which affected thousands of people, including employees and subscribers. As the actor had used The Onion Router (TOR) to mask his identity, we needed to deploy sophisticated investigative techniques and work with our partners in order to bring the investigation to a successful conclusion. Ultimately, our team was able to prevent over 300 cyber-attacks worldwide.

Operation Citiskim

As lead investigator, extensive coordination with foreign law enforcement and utilizing sophisticated investigative techniques, resulted in 14 arrests, 10 indictments, 9 convictions, spin-off investigations, millions of dollars seized in cash and property, and the first-ever criminal extradition from Estonia in the case of Aleksandr Kalinin, aka “Grig” and Nikolay Nasenkov, aka “Loader”. These two Russian nationals had conspired to hack U.S.-based financial institutions and use stolen account information to steal millions of dollars from victims’ bank accounts. Through the scheme, they had hacked an ATM network used by multiple financial institutions and stole over 800,000 accounts, causing at least

$7.8 million in losses. One of the investigative techniques I used was posing as a cooperating individual online, which led to the arrest of a leader of the criminal organization when two foreign nationals were lured to the U.S.

Gozi Malware Investigation
I led a team in prosecuting a Russian national and their cohorts for their involvement in the "Gozi" malware, which was created to evade antivirus scanners and infect over a million computers worldwide. This malware was used to steal usernames and passwords from victims' bank accounts, resulting in tens of millions of dollars in losses. The three main perpetrators were Nikita Kuzmin (known as "76"), Deniss Calovskis (known as "Miami"), and Mihai Ionut Paunescu (known as "Virus"). All three were charged in relation to the scheme.

Coletronic Computer, Inc.
Investigated and obtained the conviction of the owner of Coletronic Computer, Inc. for trafficking counterfeit Cisco products. The owner imported generic computer equipment from China that resembled Cisco networking devices, as well as packages of white stickers with CISCO model numbers, which he then marketed and sold as genuine Cisco products in the US and Europe.

Operation Trident BreACH
I formed the Money Mule Working Group (MMWG) by leveraging liaison contacts, a first of its kind collaboration between the United States Secret Service, Diplomatic Security Service, Department of Homeland Security/Homeland Security Investigations, the United States Attorney, Southern District of New York, and New York District Attorney-New York County. Cybercriminals spread the “Zeus Trojan” malware through email, which, when opened, embedded itself onto victim computers and recorded bank account numbers and passwords. From there, the criminals took control of the victim bank accounts and made unauthorized wire transfers into accounts opened by foreign actors with student visas and fake foreign passports. The MMWG was able to identify, arrest, and disrupt the activity, culminating in a cross-jurisdictional coordinated take-down that resulted in 73 actors charged, 25 convictions, and over $360,000 in restitution.

WebMoney Exchanger Investigation
I succeeded in bringing to justice a digital currency exchanger in New York who had enabled millions of dollars of illicit funds to be transferred to Russia through the conversion of those funds into WebMoney, a virtual currency with a cash equivalent.

Education

Master of Science in Information Technology (2018)
Carnegie Mellon University - Pittsburgh, PA
Graduated with Highest Distinction

Master of Business Administration (2001)
Monmouth University - West Long Branch, NJ

Bachelor of Science (1995)

Peru State College - Peru, NE

Accomplishments

New York City Federal Executive Board, Teamwork Award (2010)

- Recognized for outstanding achievement in the service of the United States Government, Operation High Rise counterterrorism investigation.

Recipient of FBI Director's Award, Outstanding Cyber Investigation (2010)

- Recognized for successfully dismantling a well-organized international cybercrime ring.

Recipient of FBI Director's Award, Outstanding Cyber Investigation (2011)

- Recognized for exemplary leadership in an innovative investigation into a prolific cybercrime enterprise.

Director of National Intelligence's Intelligence's National Intelligence Community Award for Intelligence Integration (2015)

- For my leadership in providing sustained integrated intelligence support through analytic, operational, and outreach initiatives, I was recognized for successfully neutralizing an identified threat country.

Certifications

GIAC Cloud Security Essentials Certification (GCLD), Issued, June, 2023
Certified Information Systems Security Professional (CISSP), Issued November 2021
GIAC Information Security Professional (GISP), Issued August 2020

LinkedIn Profile

[redacted]