



United States Secret Service Criminal Investigative Division

Cyber Outreach and Partnerships

The USSS Outreach Program engages private sector entities to promote USSS investigative capabilities as it relates to cyber enabled fraud and the use of illicit digital currency. This is accomplished by bringing education and awareness to the many fraud schemes surrounding cyber enabled fraud and the illicit movement of money.



Mike Johns

Director Private and Public Sector Outreach for Cyber Security
Co-Executive Director Cyber Investigative Advisory Board
U.S. Secret Service, Criminal Investigative Division

Mobile: (202) 355-3195 | **Web:** <https://www.secretservice.gov/investigation>



Brian Sevchek

Assistant to the Special Agent in Charge, Cyber Outreach Program
U.S. Secret Service, Criminal Investigative Division

Mobile: (408) 964-0681 | **Web:** <https://www.secretservice.gov/investigation>



U.S. Secret Service Global Investigative Operations Center

An integrated mission center, monitoring, coordinating, and supporting strategic domestic and international investigations with potential impact on the integrity of the financial infrastructure. The Global Investigative Operations Center (GIOC) conducts analysis of non-traditional data sources and works with our CFTFs on combating transnational organized criminal organizations.



Chris McMahon

Special Agent in Charge – Global Investigative Operations Center
U.S. Secret Service, Criminal Investigative Division

Mobile: (347) 804-1274 | **Web:** <https://www.secretservice.gov/investigation>

GIOC Resource Desks

Money Hunting Team (moneyhunting.gioc@uss.s.dhs.gov)

Supports investigations involving non-traditional financial transactions (i.e., digital and cryptocurrency payments), to include uncovering criminal identities and locating assets for potential seizure. Supports traditional financial investigations involving complex banking transaction, shell corporations, overseas trusts, straw owners, and similar aspects of money laundering schemes, by identifying assets in the U.S. and overseas. Coordinates forensic financial support for investigations requiring in-depth analysis of voluminous financial records.

Cyber Enable Crimes Desk (CyberEnabledDesk.GIOC@uss.s.dhs.gov)

Supports cyber-enabled criminal investigations, including coordinated ransomware, network intrusions, account data compromises, online sale of PII and PCI data with a focus on forums and marketplaces. This desk works closely with the Cyber Intelligence Section and Network Intrusion Responder (NITRO) Program.

Business Email Compromise Desk (BECDesk.GIOC@uss.s.dhs.gov)

Supports investigations targeting transnational Business Email Compromise (BEC) actors and their money mule networks, as well as affiliated crimes (i.e., romance scams, elder fraud, and phishing campaigns). This desk also supports investigations targeting traditional stock, insurance, Ponzi, and other general white collar bank fraud that fall under 18 U.S.C. 1344.

U.S. Secret Service Website Resources

Preparing for a Cyber Incident

<https://www.secretservice.gov/investigation/Preparing-for-a-Cyber-Incident>

- Link to Cyber Best Practices Guides in downloadable PDF accessible to the public.

U.S. Secret Service Office of Investigations

<https://www.secretservice.gov/investigation>

- USSS Office of Investigations Website

U.S. Secret Service Cyber Fraud Task Forces

<https://www.secretservice.gov/contact/field-offices>

- Contact phone numbers to USSS Field Offices



Takeaways from 1.24.23 Briefing to GFOA

- In case normal communications channels are compromised, business incident response plans must include an out-of-channel communications forum that contains up-to-date contact information for all stakeholders. Involve Law Enforcement in your incident response tabletop exercises.
- The best time to successfully recover stolen funds is often less than 48 hours. Having established a trusted relationship with Law Enforcement can help initiate the financial recovery process even before the FINCEN "kill chain" is initiated in most cases.
- No matter how small a BEC or ransomware incident is, report all cyber-enabled internet crimes to the FBI's Internet Crime Complaint Center (IC3): <https://www.ic3.gov/> or other law enforcement. Federal Law Enforcement have the ability for far reaching international investigative capabilities.
- It is extremely important to conduct regular tabletop exercises that include external partners. These tabletop exercises need to be comprehensive enough to test nuances of the incident

response plan (i.e., inclusive of details that could push the team to truly evaluate an adamant "we will always/never pay" mindset).

- It is important to include the organizational stakeholders (i.e. legal, finance and administrative employees, not just Cyber Security IT). Attorneys need to meet with the law enforcement agencies ahead of time to understand the most productive ways of working together and not creating roadblocks on either side.
- Human error and failure to report are the leading factors causing most of the cyber related incidents.
- The U.S. Secret Service have established 42 Cyber Fraud Task Forces throughout the United States and has presence in Europe with our London and Rome based Cyber Fraud Task Forces.
- The U.S. Secret Service Criminal Division has partnerships with "force multiplier" organizations such as the National Computer Forensics Institute ([NCFI](#)), the National Cyber Forensics and Training Alliance ([NCFTA](#)), and National Cyber Investigative Joint Task Force ([NCIJTF](#)).