2nd Annual Cyber and Financial Crime Conference Presentation Synopses

Breakout Session I in Alumni Hall
Social Media and Open Source Intelligence
John Sedoski, High-Tech Crime Liaison, National White Collar Crime Center (NW3C)

As criminal use of the internet becomes more and more sophisticated, law enforcement's ability to locate and act on publicly available information is more crucial than ever. Investigators must be able to turn information from varied sources into actionable intelligence as quickly and efficiently as possible. This session covers mainstream social media sites as well as third-party websites that can allow for quicker identification of potentially relevant information.

Breakout Session II in Alumni Hall
Trends in Financial Crime
Christopher Schneider, Special Agent, IRS-CI, Liaison to Financial Crimes Enforcement Network (FinCEN)

The fight against financial crime and money laundering is important to national security and the protection of the financial system in the United States. While it is a fight fought by law enforcement at the federal, state, and local levels, Bank Secrecy Act (BSA) and Anti-Money Laundering (AML) personnel are also on the front lines. This presentation will focus on the overall threats and trends in financial crime including fraud, tax evasion, public corruption, narcotics trafficking, and money laundering. Utilizing descriptions of typologies and anecdotes from real cases, the presentation will give an overview of current financial crime threats and trends.

Breakout Session IIIA: Location TDB
Fraud or Mistake: How the IRS Makes the Determination
Susan Harper, Fraud Technical Advisor, Internal Revenue Agent, Internal Revenue Service

Simple and direct, the mission of the IRS is to "provide America's taxpayers top quality service by helping them understand and meet their tax responsibilities and by applying the tax law with integrity and fairness to all." This presentation will be an overview of how the IRS meets this mission when faced with a Taxpayer who files a questionable Federal Tax Return. Is the error a mistake or an intentional one? Learn how an Internal Revenue Officer or Internal Revenue Agent identifies and develops firm indicators of fraud which serve as a sign that a Taxpayer may have taken actions for the purpose of deceit or concealment. Is a first indicator of fraud is insufficient alone to establish fraud? Learn what resources and tools the IRS utilizes to establish firm indicators of fraud needed to establish that the Taxpayer deliberately took action with the purpose of deceit, subterfuge, camouflage, or concealment. This overview will further discuss the consequences for taking such nefarious actions, including fraud penalties and/or a criminal referral to IRS Criminal Investigation, based upon the evidence. The presentation will highlight the *Dirty Dozen* tax scams.

BREAKOUT SESSION III B **Location: To be determined**

Breakout Session IIIB: Location TBD
Credential Stuffing & the Internet Fraud Alert (IFA) System
Aaron Naternicola, National Cyber Forensics & Training Alliance (NCFTA)

The focus of this presentation will be an overview of credential stealing / account stuffing and how the NCFTA's Internet Fraud Alert (IFA) system is helping to combat this ongoing threat by alerting participating organizations to their compromised credentials found stolen online.

Massive credential dumps over the past few years have led to credential stuffing becoming a serious threat to online services. Because most people reuse the same usernames and passwords across multiple platforms, attackers take massive troves of usernames and passwords and "stuff" those credentials into the login pages of other digital services. This presentation will explain how credential stuffing works and cover some of the underground markets such as Slillp & Paysell where cracked accounts are bought and sold by the thousands.

The NCFTA launched its free-of-charge IFA service in June of 2010, then revamped the system with an improved configuration and relaunch in January 2015. The IFA overview will cover the history of IFA, how the system works, and the various sources of compromised credentials provided to IFA. The overview will also review some of the massive data breaches that have been processed into IFA, statistics, and how companies may sign up to receive alerts from this service.

Breakout Session IIIC: Location TBD
On-Line Sexual Predators
Gregg Frankhouser, FBI, Pittsburgh Division, Cyber Investigation Squad
Investigations involving the exploitation of children are becoming common place. These online cyber investigations are ever changing and can be complex. On a daily basis, Detectives/Officers may receive reports of children being threatened, "sextorted", or sexually exploited while online. Reports may be made from victims and their families, from teachers or doctors, or from concerned community members. One of the most important functions of law enforcement, at that time, is to confirm the physical safety of the child. Law enforcement's role however, doesn't end at the initial call. Perhaps there's concern for the child running away or being physically removed by an offender. Law enforcement may play a crucial part in providing guidance and support to the child/family as well.

This presentation will provide information to law enforcement officials on how to triage investigations, preserve online information, obtain online information via search warrant or subpoena, and provide advice on best practices for conducting searches. Other items discussed include securing cellular telephones for forensic processing and conducting a forensic review of digital evidence. While these types of investigations can be overwhelming, by connecting each smaller piece of the investigation, a larger, more understandable investigative process will emerge.

When Law Enforcement protects our children from criminal predators, they are protecting and serving their community as well with the arrest of those offenders.

Breakout Session IV in Alumni Hall
Association of Certified Fraud Examiners *2018 Report to the Nations*
Laura Hymes, CFE, Program Manager, Association of Certified Fraud Examiners, Austin, TX

This session will introduce key findings from the Association of Certified Fraud Examiners' 2018 *Report to the Nations*. We will discuss overall trends in the report and then dive deeper into findings about scheme types, statistical characteristics of fraud perpetrators, and red flags that might indicate fraudulent behavior. Discover what types of fraud are the most common and various detection methods that can successfully uncover fraud. You will also learn how to benchmark your anti-fraud efforts against similar organizations and against the most effective methods for reducing fraud losses.

Breakout Session V in Alumni Hall
Use of Bank Secrecy Act (BSA) Data by Law Enforcement
Christopher Schneider, Special Agent, IRS, Criminal Investigation, Liaison to FinCEN

As one of the primary users of BSA data, law enforcement knows the value BSA data can bring to an investigation. This presentation will focus on the use of Bank Secrecy Act (BSA) Data by law enforcement, with a particular emphasis on how IRS-CI uses BSA data to carry out its mission. Presentation topics include trends in BSA filing, an overview of the law enforcement audience for BSA data, why BSA data is valuable to law enforcement, the different approaches to using BSA data (reactive vs. proactive), and Suspicious Activity Report (SAR) writing tips from the law enforcement perspective.