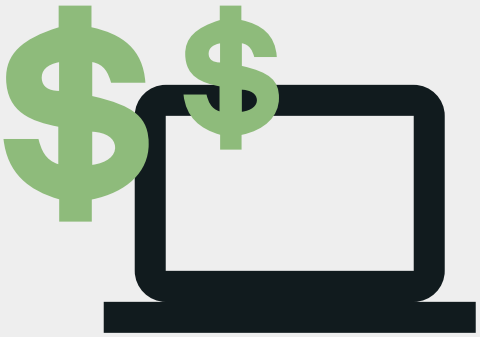

SECOND ANNUAL

Cyber and Financial Crime Conference

HOSTED BY

WAYNESBURG UNIVERSITY

THURSDAY, MARCH 28, 2019
8:30 A.M. - 4 P.M.
WAYNESBURG UNIVERSITY
51 W. COLLEGE ST., WAYNESBURG, PA. 15370

Event Schedule

8:30 a.m. - 9:30 a.m. - Registration/Meet & Greet (Continental Breakfast Provided)
Benedum Dining Hall, Waynesburg University

9:30 a.m. - 9:40 a.m. - Introduction & Opening Remarks by Provost Dana Baer

9:50 a.m. - 10:40 a.m. - Social Media & Open Source Intelligence

10:50 a.m. - 11:40 a.m. - Trends in Financial Crime

11:40 a.m. - Noon - Break

Noon - 12:50 p.m. - Breakout Sessions (Choose from one of three options)

1 p.m. - 2 p.m. - Buffet-style Lunch

2 p.m. - 2:50 p.m. - Association of Certified Fraud Examiners 2018 Report to the Nations

3 p.m. - 3:50 p.m. - Use of Bank Secrecy Act Data by Law Enforcement

3:50 p.m. - 4 p.m. - Wrap Up

Sessions

Session I, Alumni Hall

Social Media & 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.

Session II, 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.

Session III, Group A, Location TBD

Fraud or Mistake: How the IRS Makes the Determination

Susan Harper, Fraud Technical Advisor, Internal Revenue Agent, IRS

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.

Session III, Group B, 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.

Session III, Group C, Location TBD - Law Enforcement Professionals ONLY

Online 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.

Session IV, 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.

Session III, 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 Bank Secrecy Act 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.

Organization Descriptions

Association of Certified Fraud Examiners (ACFE)

The ACFE is the world's largest anti-fraud organization and premier provider of anti-fraud training, education, and certification. Together with nearly 85,000 members, the ACFE is reducing business fraud world-wide and inspiring public confidence in the integrity and objectivity within the profession.

The mission of the Association of Certified Fraud Examiners is to reduce the incidence of fraud and white-collar crime and to assist the Membership in fraud detection and deterrence. The Certified Fraud Examiner (CFE) credential denotes proven expertise in fraud prevention, detection and deterrence. CFEs are trained to identify the warning signs and red flags that indicate evidence of fraud and fraud risk. CFEs around the world help protect the global economy by uncovering fraud and implementing processes to prevent fraud from occurring in the first place.

CFEs have a unique set of skills that are not found in any other career field or discipline; they combine knowledge of complex financial transactions with an understanding of methods, law, and how to resolve allegations of fraud.

Financial Crime Enforcement Network (FinCEN)

FinCEN is a bureau of the U.S. Department of the Treasury. FinCEN's mission is to safeguard the financial system from illicit use and combat money laundering and promote national security through the collection, analysis, and dissemination of financial intelligence and strategic use of financial authorities. FinCEN carries out its mission by receiving and maintaining financial transactions data; analyzing and disseminating that data for law enforcement purposes; and building global cooperation with counterpart organizations in other countries and with international bodies.

FinCEN exercises regulatory functions primarily under the Currency and Financial Transactions Reporting Act of 1970, as amended by Title III of the USA PATRIOT Act of 2001 and other legislation, which legislative framework is commonly referred to as the "Bank Secrecy Act" (BSA).

The BSA is the nation's first and most comprehensive Federal anti-money laundering and counter-terrorism financing (AML/CFT) statute. In brief, the BSA authorizes the Secretary of the Treasury to issue regulations requiring banks and other financial institutions to take a number of precautions against financial crime, including the establishment of AML programs and the filing of reports that have been determined to have a high degree of usefulness in criminal, tax, and regulatory investigations and proceedings, and certain intelligence and counter-terrorism matters.

National Cyber Forensic Training Alliance (NCFTA)

The National Cyber-Forensics & Training Alliance (NCFTA) is a non-profit corporation founded in 2002, focused on identifying, mitigating, and neutralizing cybercrime threats globally. The NCFTA operates by conducting real-time information sharing and analysis with Subject Matter Experts (SME) in the public, private, and academic sectors. Through these partnerships, the NCFTA proactively identifies cyber threats in order to help partners take preventive measures to mitigate those threats. The NCFTA has a proven track record and has long been identified as the model for private/public partnerships. Today, the NCFTA model, best practices, and lessons learned are being leveraged and emulated in countries around the world. NCFTA membership is constantly growing both nationally and internationally across private industry, law enforcement, government, and academia.

National White Collar Crime Center (NW3C)

NW3C is a nonprofit, membership-affiliated organization comprised of state, local, federal and tribal law enforcement and prosecutorial and regulatory agencies. NW3C provides a nationwide support system for law enforcement and regulatory agencies involved in the prevention, investigation and prosecution of economic and high-tech crime. We deliver training in computer forensics, cyber and financial crime investigations and intelligence analysis. We offer analytical technical support to agencies investigating and prosecuting white collar and related crimes. We conduct original research on all facets of white collar crime.

For more than three decades, the National White Collar Crime Center has worked to support state and local law enforcement efforts to prevent, investigate and prosecute economic and high-tech crime.

The NW3C serves as a means to link criminal justice agencies across jurisdictional borders. NW3C provides support for the prevention, investigation, and prosecution of economic and high-tech crime through a combination of research, training, and investigative support services. Since its establishment, NW3C has progressively strengthened its commitment to its members and mission. Today, NW3C has more than 5, 000 member agencies in the U.S. and its territories as well as 15 other countries throughout the world.

Speaker Biographies

Gregg Frankhouser, Special Agent, Federal Bureau of Investigations, Cyber Investigation Squad

FBI Special Agent Gregg Frankhouser has been with the FBI for 17 years in the New York and Pittsburgh Divisions. Gregg is currently assigned to the Cyber Investigations Squad, responsible for investigating matters related to Crimes Against Children. He is certified to conduct forensic processing and analysis of digital devices as a Digital Extraction Technician (DEXT). Gregg also holds the following certifications: A+ Computer Hardware Certification; Basic Data Recovery and Analysis (BDRA) and Microsoft Certified Systems Engineer (MCSE). In New York he was assigned to Special Operations Division, Computer Analysis Response Team (CART) as Forensic Examiner and to the Criminal Division, White Collar Crimes Branch, where he conducted Computer Crime/Fraud Investigations.

Susan Harper, Internal Revenue Agent Fraud Technical Advisor, IRS

Internal Revenue Agent Susan Harper has been with the IRS for nearly 32 years in Pittsburgh, Pennsylvania, and Bridgeport, West Virginia. Susan is currently a Fraud Technical Advisor (since 2008) serving as a liaison for Criminal Investigation and all Civil functions of the IRS, including but not limited to Small Business Self-Employed (SBSE), Large Business & International (LB&I), as well as Specialty Groups including Tax Exempt/Government Entities (TEGE), Employment Tax, Excise Tax, and Estate/Gift Tax. In this role, Susan educates her civil function customers on the identification and development of indicators of fraud to support fraud penalties and/or criminal referral recommendations. In 1988, Susan graduated summa cum laude from Fairmont State University and is an owner of Pennsylvania Tax Institutes Inc. (PTI). Susan not only instructs each fall for PTI to CPAs, Enrolled Agents, Certified Financial Planners, and attorneys who enroll to obtain CPE credits, but also instructs two 2-day seminars for West Virginia University in the same subject matter.

Laura Hymes, CFE, Program Manager, Association of Certified Fraud Examiners (ACFE), Austin, TX

Laura Hymes, CFE, is the Program Manager for the Association of Certified Fraud Examiners (ACFE), where she develops the educational lineup for ACFE conferences held around the world. She works closely with subject-matter experts to provide educational content for anti-fraud professionals of all skill and experience level.

In addition to working with outside experts, Laura is part of the Research Department at the ACFE. In that role, she helps research, write, and edit training materials related to the prevention, deterrence, and detection of fraud. She has co-edited books in Dr. Joseph T. Wells's Fraud Casebook series and has written numerous anti-fraud articles for industry publications.Prior to joining the staff of the ACFE, Hymes worked as an editor and project manager in the educational-publishing industry. She earned a Bachelor of Arts in English from the University of Texas at Austin. She also holds a Master of Science in Publication Management from Drexel University in Philadelphia, Pennsylvania.

Aaron Naternicola, Intelligence Analyst, National Cyber Forensic & Training Alliance (NCFTA)

Aaron is a senior level Intelligence Analyst for the NCFTA embedded at the FBI's Internet Crime Complaint Center (IC3). For the past seven years, he has managed the NCFTA's Internet Fraud Alert (IFA) system, a central repository and alerting mechanism for compromised credentials found stolen online – payment cards, email accounts, & user/login accounts. Prior to joining the NCFTA, he spent 10 years as a senior level analyst for the National White Collar Crime Center (NW3C) compiling Internet crime cases for state and local law enforcement across the country. Aaron graduated from nearby Fairmont State University with a Bachelor Degree in Engineering Technology.

Christopher Schneider, Special Agent, IRS, Criminal Investigation, Liaison to FinCEN

IRS-CI Special Agent (SA) Chris Schneider has been with the IRS-CI since 2009. During his career, SA Schneider has investigated cases involving criminal tax, fraud, narcotics, and money laundering violations. SA Schneider is currently

assigned to IRS-CI headquarters as IRS-CI's liaison to the Financial Crimes Enforcement Network (FinCEN). Prior to joining IRS-CI, SA Schneider worked for Ernst & Young in its Fraud Investigation and Dispute Services practice. SA Schneider is a Certified Public Accountant (CPA) and a Certified Fraud Examiner (CFE). SA Schneider graduated from Wake Forest University with a Bachelor's degree in Analytical Finance and a Master's degree in Accountancy.

John Sedoski, High-Tech Crime Liaison, National White Collar Crime Center (NW3C)

John Sedoski is currently serving as the High-Tech Crime Liaison with the National White Collar Crime Center (NW3C). Mr. Sedoski joined NW3C in the fall of 2010 as a Computer Crimes Specialist. John has provided thousands of hours of training to numerous state, local, and federal law enforcement personnel in data recovery and analysis. Training topics range from basic identifying and seizing electronic evidence, analysis of artifacts Operating Systems, and to an ever-evolving field of Social Media investigations. John is also a Certified Forensic Computer Examiner (CFCE) and has served on his local HTCIA board.

John has provided technical assistance to law enforcement personnel on computer/cyber forensic topics, lead and participated in curriculum development for NW3C classes by researching course topics, preparing presentations and class materials and developing hands-on projects. Additionally, Mr. Sedoski has also participated in the research and validation of software programs developed by NW3C and conducted original research on forensic topics relating to the application of computer forensic methods.

John earned a B.S. from West Virginia University, majoring in Computer and Electrical Engineering. During this time, he worked in the West Virginia State Police Digital Forensic Lab where he was able to provide aid by using his education and applying it to the field of computer forensics.