WEDNESDAY	
08:00 – 09:00 AM	Breakfast MCCONE
09:00 – 09:10 AM	Opening Remarks: Moyara Ruehsen IRVINE AUDITORIUM
09:10 – 10:10 AM	**Cybersecurity & Partnering with The FBI** Presenter: Special Agent Enrique M. Alvarez (FBI San Francisco, Cyber Branch) Special Agent Alvarez of the FBI Cyber Unit will discuss trending cybersecurity issues, how the FBI investigates cyber intrusion, what are the US Government's cybersecurity responsibilities, the scope of the cyber threat, attack vectors, who's doing the hacking, and how the FBI investigates cyber incidents. IRVINE AUDITORIUM
10:10 – 10:50 AM	**PANEL: Public Private Partnerships** *Moderator: B. Andy Stewart* *Panelists: Jim Dinkins (President, Thomson Reuters Special Services), Yaya Fanusie (CNAS), Enrique Alvarez (FBI), and Pam Clegg (Ciphertrace)* As technology and regulations change at a rapid pace and criminals adapt to new enforcement regimes, the public and private sector must continue to develop partnerships and enhance real time collaboration to mitigate systemic risk to the U.S. financial system. Moderator Andy Stewart will interview Jim Dinkins, the President of Thomson Reuters Special Services (and formerly with HSI) about how TRSS works with the intelligence community; Yaya Fanusie, one of the world's foremost terrorism financing experts and a former CIA analyst, who personally briefed President George W. Bush on terrorist threats; and Special Agent Alvarez from the FBI's Cyber Unit. IRVINE AUDITORIUM
10:50 – 11:10 AM	Networking Break
11:10 – 11:50 PM	**Online Fraud: Protecting against Synthetic Identities and Account Takeovers** *Presenter: Jennifer Singh, Entersekt* Where there's money being exchanged for goods, there's also fraud. A lot of it. Criminals are following closely behind as the global economy shifts online. Every day, they conduct elaborate schemes that significantly impact financial institutions, retailers, all of us. During this session, we will discuss trends in digital fraud and the impact it is having on key industries. We will explore how fraudsters utilize attack vectors, including synthetic identities and account takeover attacks, to defraud their targets and weaponize their stolen personal data. IRVINE AUDITORIUM

11:50 – 12:30 PM	**PANEL: Preventing Cyber Fraud** *Moderator: B. Andy Stewart* *Panelists: David Zacks (Bitflyer), Vikas Agarwal (PwC), Jennifer Singh (Entersekt)* Moderator Andy Stewart discusses with Jennifer Singh some of the new tactics that can mitigate against synthetic identities and account takeovers, with the aim of leaving you better prepared to protect your digital channels from criminal activity. He will also discuss with David Zacks, the Chief Compliance Officer at Bitflyer, how the customer onboarding process can be modified to prevent fraud, and the kinds of technology financial institutions need to prevent fraud. IRVINE AUDITORIUM
12:30 – 01:30 PM	Lunch SAMSON CENTER
01:30 – 02:45 PM	<u>BREAKOUT WORKSHOPS</u> **OPTION 1: Typologies and Benchmarks: How Financial Institutions can use data to assess Risks and Opportunities in Cryptocurrency** *Presenter: Alex Rawitz (Chainalysis)* Alex Rawitz will walk attendees through some of the basic typologies in the cryptocurrency space, including case studies showing how cryptocurrencies are used in threat financing and other illicit activities. Next, he'll extrapolate from individual examples to industry-wide statistics on illicit activity, using Chainalysis data to illustrate the landscape of economic activity and money laundering across cryptocurrencies. Finally, he'll talk about how financial institutions should think about using this data to assess current and future risks and opportunities in this space. **OPTION 2: The Evolution of Cryptocurrencies** *Presenter: Sam Whitefield (MIIS)* From humble origins in 2009, cryptocurrency has become an important factor across the world of finance. This talk charts the evolution of the crypto space along three different axes--the increasing maturity of cryptocurrency markets, the myriad technological forms built upon the basic foundation of peer-to-peer electronic money, and the prevalence of various types of scams aimed at separating low-information participants from their (digital) wallets. **OPTION 3: New Breakthroughs in Negative News** *Presenters: Yelena Shapiro and Spencer Torene (Thomson Reuters Special Services)* Regulatory requirements around news monitoring are cumbersome. The necessary reviews, cross-checks, and analysis of media reporting can take thousands of hours away from critical investigations. New tools for adverse media screening are changing the game, with significant time and cost savings. Join us for a lively conversation where we'll dive into the latest trends in risk detection, modeling, and taxonomy, not to mention the challenge of false positives. We'll also share real-world examples of the opportunities inherent in machine learning (ML) and Natural Language Processing (NLP). If you're ready for a new way to approach risk intelligence, or just looking to streamline your compliance workflows, this session is for you. **OPTION 4: The Rise of Crypto MSBs** *Presenter: Joules Barragan (Ciphertrace)* Join us for a series of case studies and new research documenting the different ways criminals abuse cryptocurrencies. From the rise of illicit crypto money service businesses to dark markets to terrorism financing, learn how cryptocurrency threat intelligence and blockchain forensics helps law enforcement and financial institutions identify and stop bad actors.
02:45 – 03:05 PM	Networking Break

03:05 – 03:50 PM	**Nation-State Exploitation of Cryptocurrencies** *Presenter: Liat Shetret, Elliptic* Cryptocurrencies are enabling nation-states to evade sanctions, raise funds and engage in cyberwarfare. In this session we will explain how cryptocurrencies are being used by nation-states to promote their agendas and project influence and power beyond their borders, and how blockchain analysis can be used to gain new insights into these activities. Examples will include Russia, Iran, Venezuela, and North Korea. IRVINE AUDITORIUM
03:50 – 04:10 PM	**CASE STUDY: Sanctions Evasion Goes Digital** *Presenter: Cameron Trainer, MIIS-CNS* This presentation will explore how entities in North Korea's IT sector have transitioned to e-commerce as a means of engaging in trade otherwise restricted through multilateral and unilateral sanctions regimes. In particular, this presentation will pull from a range of work conducted by the James Martin Center for Nonproliferation Studies (CNS) to highlight the difficulties in identifying North Korean actors on digital platforms. The presentation will increase the ability of audience members to comply with regulations relating to the prevention, suppression and disruption of proliferation of weapons of mass destruction and its financing. IRVINE AUDITORIUM
04:10 – 04:25 PM	**CASE STUDY: North Korean ICO Scams** *Presenter: Sam Whitefield, MIIS* One of the newest methods the Kim regime has used to acquire hard currency is the sale of fraudulent cryptocurrencies. This talk explains why the North Koreans are engaging in crypto scams, and details the two known case studies where this tactic has been used. IRVINE AUDITORIUM
4:25 – 05:00 PM	**PANEL: Crypto Rogues** *Moderator: Yaya Fanusie (CNAS)* *Panelists: Liat Shetret (Elliptic), Cameron Trainer (CNS), Samuel Whitefield (MIIS)* This panel will discuss how cryptocurrencies and blockchain technology more broadly are impacting the geopolitical and international security landscape. Panelists will discuss how countries seeking to skirt sanctions are leveraging new financial technology and assess the likelihood that these alternative means for transferring value could threaten the current AML and sanctions regulatory framework. IRVINE AUDITORIUM
05:00 – 07:00 PM	Networking Reception SAMSON CENTER

THURSDAY	
08:00 – 09:00 AM	Breakfast MCCONE
09:00 – 09:45 AM	**2020 State of Crypto Crime** *Presenter: Jonathan Levin (Cofounder & CSO at Chainalysis)* In this session, Jonathan Levin, Co-Founder and Chief Strategy Officer, Chainalysis, breaks down the latest trends in crypto crime, including why 2019 was the year of the ponzi scheme, the role of corrupt OTC brokers in money laundering, how hackers evolved their strategies, and more. IRVINE AUDITORIUM
09:45 – 10:45 AM	**How to Build a Criminal Case Involving Cryptocurrencies** *Presenter: Lourdes Miranda (Miranda FinIntel)* Learn what to include and look for in Suspicious Activity Reporting (SARs) and Currency Transaction Reporting (CTRs); what are the advantages and disadvantages of building the chain of custody on the blockchain; and, understand the value of investigative and analytical cryptocurrency and blockchain tools when building criminal cases. IRVINE AUDITORIUM
10:45 – 11:05 AM	Networking Break
11:05 – 11:50 AM	**Ransomware Goes Nuclear** *Presenter: Roger Grimes (KnowBe4)* There is a reason more than half of today's ransomware victims end up paying the ransom. Cyber-criminals have become thoughtful; taking time to maximize your organization's potential damage and their payoff. After achieving root access, the bad guys explore your network reading email, finding data troves and once they know you, they craft a plan to cause the most panic, pain, and operational disruption. In this presentation Roger Grimes, KnowBe4's Data-Driven Defense Evangelist, will dive into why data backups (even offline backups) won't save you, how threats have evolved from data-theft, credential leaks, and corporate impersonation, why ransomware isn't your real problem, and how your end users can become your best, last line of defense. IRVINE AUDITORIUM
11:50 – 01:00 PM	**PANEL: Blurred Lines: Ransomware & Its Impact on Cyberinsurance** *Moderator: Thomas (Thom) Yohannan – Aon Cyber Solutions* *Panelists: Roger Grimes (KnowBe4), Jasmine Sturdifen (MIIS), Josh Motta (Coalition, Inc.), and Debra Brown (Chainalysis)* Ransomware, business interruption, compromised vendors, nation-state attacks – cyber claims run the gamut of risks. The emerging threat landscape will challenge information security and cyber insurance professionals in the coming months and years. This session will feature a wide-ranging discussion on determining the financial impact of ransomware, the growing sophistication of ransomware, and social engineering attacks, the difficulties inherent in attack attribution, as well as cyber coverage concepts. IRVINE AUDITORIUM
01:00 – 02:00 PM	Lunch SAMSON CENTER

02:00 – 03:15 PM	BREAKOUT WORKSHOPS

OPTION 1: Typologies and Benchmarks: How Financial Institutions can use data to assess Risks and Opportunities in Cryptocurrency

Presenter: Alex Rawitz (Chainalysis)

Alex Rawitz will walk attendees through some of the basic typologies in the cryptocurrency space, including case studies showing how cryptocurrencies are used in threat financing and other illicit activities. Next, he'll extrapolate from individual examples to industry-wide statistics on illicit activity, using Chainalysis data to illustrate the landscape of economic activity and money laundering across cryptocurrencies. Finally, he'll talk about how financial institutions should think about using this data to assess current and future risks and opportunities in this space.

OPTION 2: The Evolution of Cryptocurrencies

Presenter: Sam Whitefield (MIIS)

From humble origins in 2009, cryptocurrency has become an important factor across the world of finance. This talk charts the evolution of the crypto space along three different axes--the increasing maturity of cryptocurrency markets, the myriad technological forms built upon the basic foundation of peer-to-peer electronic money, and the prevalence of various types of scams aimed at separating low-information participants from their (digital) wallets.

OPTION 3: Social Clues: Understanding the Role and Capability of Social Media in AML and CFT Investigations

Presenter: Chad Longo (Thomson Reuters Special Services)

Chad Longo will explore various methods for collecting and observing information in open sources and social media to augment AML and CFT investigations. Criminal enterprises may also leverage social platforms to enable informal transfer networks, which can be observed with proper collection and analysis. We will work through several case examples to help participants gain skills necessary to conduct more advanced investigations with non-traditional resources.

OPTION 4: The Rise of Crypto MSBs

Presenter: Joules Barragan (Ciphertrace)

Join us for a series of case studies and new research documenting the different ways criminals abuse cryptocurrencies. From the rise of illicit crypto money service businesses to dark markets to terrorism financing, learn how cryptocurrency threat intelligence and blockchain forensics helps law enforcement and financial institutions identify and stop bad actors.

03:15 – 03:30 PM	Networking Break
03:30 – 03:45 PM	**CASE STUDY: SamSam Ransomware**

Presenter: Alice Saltini (MIIS)

This brief case examination delves into the effects of the deployment of one variant of SamSam Ransomware. Deployed in 2015 by two Iranian nationals. This ransomware struck critical infrastructure, including municipalities and hospitals, and affected more than 200 victims worldwide. The attacks generated $6 million in Bitcoin ransom payment, processed through two Iranian exchanges, and led to roughly $30 million in damages for the affected victims.

IRVINE AUDITORIUM

03:45 – 05:00 PM	**PANEL: Money Laundering on Online Gaming Platforms** *Moderator: Connor Freeman (Wells Fargo)* *Panelists: Emily Stonehouse (Linden Lab), Kelly Conway (Manticore Games), and Alex Newhouse (CTEC)* After first describing how online games can be used for money laundering, this panel discussion will explore the cybercrime risks of in-world currencies / digital assets, and how to create AML/ Fraud monitoring and KYC programs while not deterring legitimate players from the games. IRVINE AUDITORIUM
05:00 – 07:00 PM	Networking Reception MARRIOT HOTEL

FRIDAY

08:00 – 09:00 AM	Breakfast MCCONE
09:00 – 09:40 AM	**Why Crypto Threat Intelligence Should Be Integrated Into Bank Operations** *Presenter: Pam Clegg (Ciphertrace)* Criminals funnel illegal gains through hundreds of unregulated cryptocurrency service businesses and into the banking system. Yet this cryptocurrency activity frequently goes unnoticed in the ACH, SWIFT, wire, and credit card payment networks. This session will give you actionable information on how cryptocurrency threat intelligence can be integrated into bank operations to give increased visibility into criminal actors, detect unregistered and illicit cryptocurrency businesses that may be using accounts at your bank, and understand how to appropriately conduct CDD/EDD on customers buying/selling cryptocurrencies. IRVINE AUDITORIUM
09:40 – 10:30 AM	**Terrorists Raising their Crypto IQ through Experimentation and Adaptation** *Presenter: Yaya Fanusie (CNAS)* Yaya J. Fanusie, a former analyst with the CIA, has been researching terrorism financing for decades, and specifically terrorists' cryptocurrency fundraising since 2016. In this session, he will discuss case studies of various jihadist groups who have run cryptocurrency crowdfunding campaigns, explain how they are sharpening their tools and techniques, and point out ways to address the regulatory and security challenges as terrorists adapt. IRVINE AUDITORIUM
10:30 – 10: 50 AM	Networking Break
10:50 – 11:20 AM	**Money Laundering and Terrorism Financing Risks using Cryptocurrency ATMs** *Presenter: Lourdes Miranda (Miranda FinIntel)* This session explores the money laundering and terrorist financing threats involving Bitcoin / Crypto Automated Teller Machines (BTMs / CTMs); how to mitigate those threats; what are the reporting requirements for money services businesses; how to build criminal cases; and which investigative and analytical tools are recommended. IRVINE AUDITORIUM

11:20 – 12:20 PM	**Diabolical Phishing Schemes** *Presenter: Michael Manrod (CISO, Grand Canyon Education)* Every year, billions of dollars are spent hardening systems to prevent exploitation by malicious parties wanting to steal, ransom or destroy valuable information / systems. However, the one system that remains difficult to patch is the human mind. In this talk we will look at latest phishing techniques and how attackers evade both technology systems and entice people to cooperate unknowingly with an attack. IRVINE AUDITORIUM
12:20 – 12:30 PM	Closing Remarks: Moyara Ruehsen IRVINE AUDITORIUM
12:30 – 01:30 PM	Lunch SAMSON CENTER