U.S. Secret Service

Cyber Fraud Task Force Bulletin

Sharing News Among Our Law Enforcement and Industry Partners

January 2021

Inside This Edition

CURRENT TRENDS & RESOURCES

BLUETOOTH SKIMMING DETECTION

The U.S. Secret Service San Diego Field Office and a team of computer scientists at the University of California - San Diego and the University of Illinois developed an Android compatible application - Bluetana - that allows investigators to detect Bluetooth skimming devices installed in gas pumps. Bluetana identifies broadcasting Bluetooth devices and flags suspicious Bluetooth emitters which are likely to be Bluetooth enabled skimmers.

The researchers found that, compared to similar apps currently available for smartphones, Bluetana is likely to discover more skimmers and results in a much lower false positive rate. Bluetana uses an algorithm developed by the researchers to distinguish skimmers from legitimate Bluetooth devices.

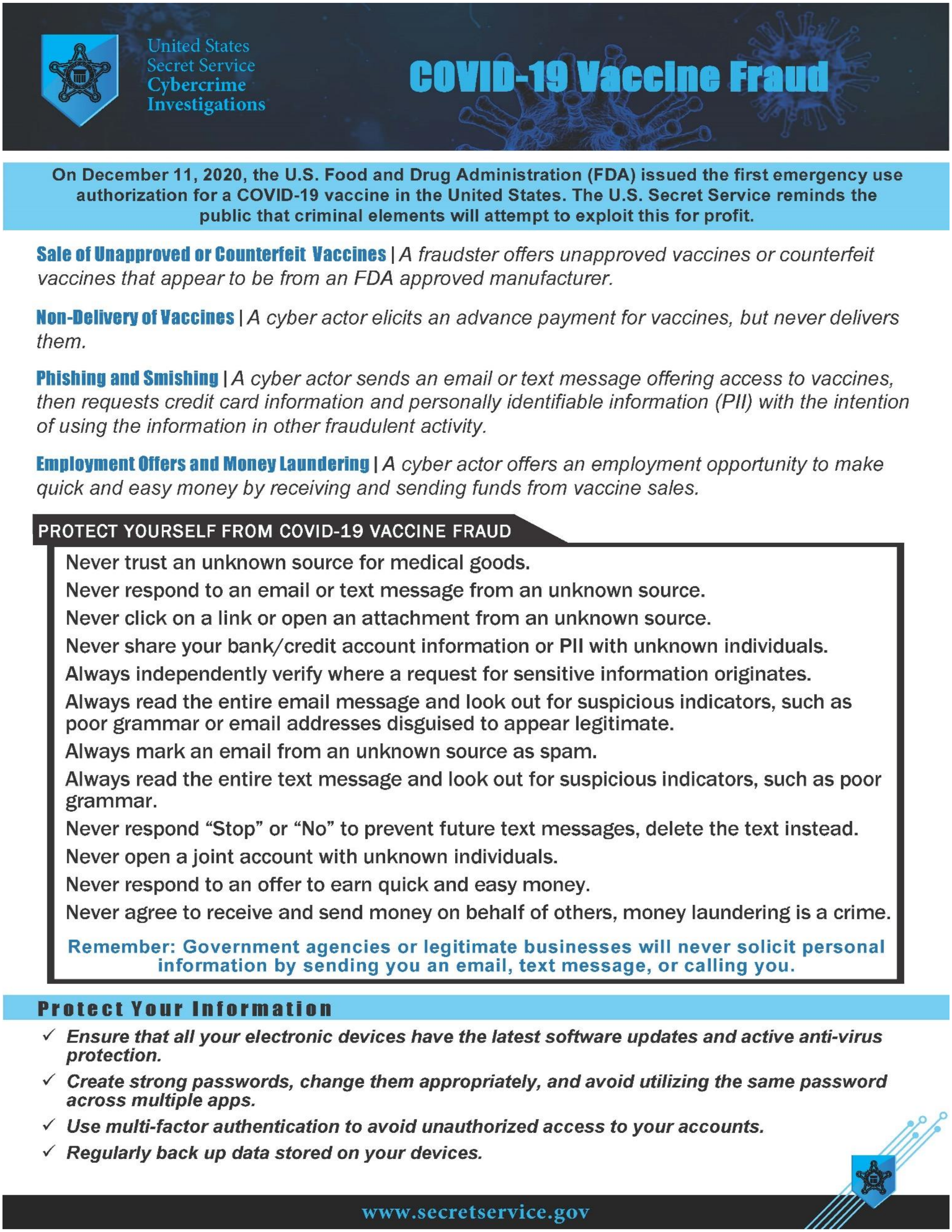
Bluetana is available to Secret Service Cyber Fraud Task Force (CFTF) law enforcement partners. Investigators should speak with their Computer Hacking and Intellectual Property (CHIP) Assistant U.S. Attorney or state prosecutor before utilizing Bluetana. If approved for use by an Assistant U.S. Attorney or state prosecutor, investigators should purchase an Android phone (Motorola G2/E3 or better) and contact the Secret Service San Diego Field Office based SoCal CFTF at SOCAL-CFTF@usss.dhs.gov.

FinCEN ASKS FINANCIAL INSTITUTIONS TO STAY ALERT TO COVID-19 VACCINE-RELATED SCAMS AND CYBERATTACKS

The Financial Crimes Enforcement Network (FinCEN) issued a notice to alert financial institutions about the potential for fraud, ransomware attacks, or similar types of criminal activity related to COVID-19 vaccines and their distribution. This notice also provides specific instructions for filing Suspicious Activity Reports (SARs) regarding such suspicious activity related to COVID-19 vaccines and their distribution.

Notice: https://www.fincen.gov/sites/default/files/shared/COVID-19%20Vaccine%20Notice%20508.pdf

SECRET SERVICE WARNS CONSUMERS OF FRAUD RELATED TO COVID-19 VACCINES



United States
Secret Service
Cybercrime
Investigations

COVID-19 Vaccine Fraud

On December 11, 2020, the U.S. Food and Drug Administration (FDA) issued the first emergency use authorization for a COVID-19 vaccine in the United States. The U.S. Secret Service reminds the public that criminal elements will attempt to exploit this for profit.

Sale of Unapproved or Counterfeit Vaccines | *A fraudster offers unapproved vaccines or counterfeit vaccines that appear to be from an FDA approved manufacturer.*

Non-Delivery of Vaccines | *A cyber actor elicits an advance payment for vaccines, but never delivers them.*

Phishing and Smishing | *A cyber actor sends an email or text message offering access to vaccines, then requests credit card information and personally identifiable information (PII) with the intention of using the information in other fraudulent activity.*

Employment Offers and Money Laundering | *A cyber actor offers an employment opportunity to make quick and easy money by receiving and sending funds from vaccine sales.*

PROTECT YOURSELF FROM COVID-19 VACCINE FRAUD

Never trust an unknown source for medical goods.

Never respond to an email or text message from an unknown source.

Never click on a link or open an attachment from an unknown source.

Never share your bank/credit account information or PII with unknown individuals.

Always independently verify where a request for sensitive information originates.

Always read the entire email message and look out for suspicious indicators, such as poor grammar or email addresses disguised to appear legitimate.

Always mark an email from an unknown source as spam.

Always read the entire text message and look out for suspicious indicators, such as poor grammar.

Never respond “Stop” or “No” to prevent future text messages, delete the text instead.

Never open a joint account with unknown individuals.

Never respond to an offer to earn quick and easy money.

Never agree to receive and send money on behalf of others, money laundering is a crime.

Remember: Government agencies or legitimate businesses will never solicit personal information by sending you an email, text message, or calling you.

Protect Your Information

- ✓ ***Ensure that all your electronic devices have the latest software updates and active anti-virus protection.***
- ✓ ***Create strong passwords, change them appropriately, and avoid utilizing the same password across multiple apps.***
- ✓ ***Use multi-factor authentication to avoid unauthorized access to your accounts.***
- ✓ ***Regularly back up data stored on your devices.***

www.secretservice.gov

SECRET SERVICE ISSUES URGENT ALERT FOR E-COMMERCE VENDORS

The Secret Service has detected a significant upsurge in e-Skimming attacks due to an increase in online shopping.

E-Skimming

E-Skimming targets businesses accepting online payments. Often called “Magecart” attacks by researchers, cybercriminals leverage vulnerabilities, known and unknown, to modify stores’ source code to steal payment card data in real time.

Magento Platform

The Secret Service specifically noted a campaign targeting online stores running legacy versions of the open source e-commerce platform Magento. All versions of Magento 1 are considered end-of-life (EOL) as of June 30, 2020, meaning no further vendor security patches are forthcoming. Magento still provides support for its Open Source 2 product. An estimated 75,000 live sites are currently operating on Magento 1 platforms, highlighting the target-rich environment that exists for cybercriminals looking to take advantage of the ease and high profitability of e-skimming.

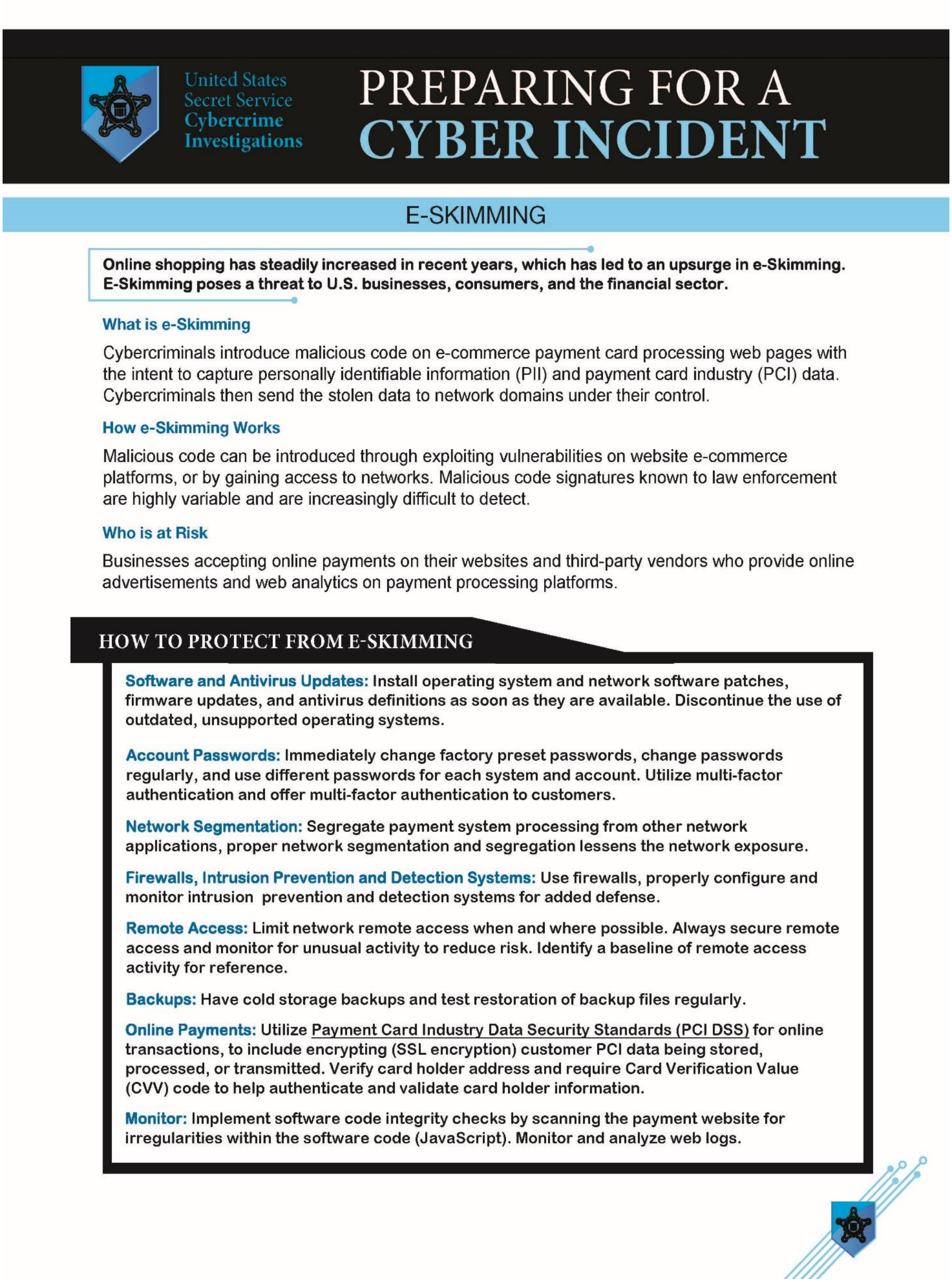
Recommended Risk Mitigations

- Keep all systems patched and up-to-date, to include operating systems, software, and any third-party code running as part of your website.
- Do not use default login credentials on any system.
- Keep web application firewalls strong and monitor administrative activity.
- Eliminate/disable functions within your online store that are not necessary.
- Monitor requests performed against your store’s environment to identify possible malicious activity (loader and exfiltration domains).

Contact your local U.S. Secret Service field office Cyber Fraud Task Force (CFTF).

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

SECRET SERVICE PUBLISHES e-SKIMMING GUIDE



United States
Secret Service
**Cybercrime
Investigations**

PREPARING FOR A CYBER INCIDENT

E-SKIMMING

Online shopping has steadily increased in recent years, which has led to an upsurge in e-Skimming. E-Skimming poses a threat to U.S. businesses, consumers, and the financial sector.

What is e-Skimming

Cybercriminals introduce malicious code on e-commerce payment card processing web pages with the intent to capture personally identifiable information (PII) and payment card industry (PCI) data. Cybercriminals then send the stolen data to network domains under their control.

How e-Skimming Works

Malicious code can be introduced through exploiting vulnerabilities on website e-commerce platforms, or by gaining access to networks. Malicious code signatures known to law enforcement are highly variable and are increasingly difficult to detect.

Who is at Risk

Businesses accepting online payments on their websites and third-party vendors who provide online advertisements and web analytics on payment processing platforms.

HOW TO PROTECT FROM E-SKIMMING

Software and Antivirus Updates: Install operating system and network software patches, firmware updates, and antivirus definitions as soon as they are available. Discontinue the use of outdated, unsupported operating systems.

Account Passwords: Immediately change factory preset passwords, change passwords regularly, and use different passwords for each system and account. Utilize multi-factor authentication and offer multi-factor authentication to customers.

Network Segmentation: Segregate payment system processing from other network applications, proper network segmentation and segregation lessens the network exposure.

Firewalls, Intrusion Prevention and Detection Systems: Use firewalls, properly configure and monitor intrusion prevention and detection systems for added defense.

Remote Access: Limit network remote access when and where possible. Always secure remote access and monitor for unusual activity to reduce risk. Identify a baseline of remote access activity for reference.

Backups: Have cold storage backups and test restoration of backup files regularly.

Online Payments: Utilize Payment Card Industry Data Security Standards (PCI DSS) for online transactions, to include encrypting (SSL encryption) customer PCI data being stored, processed, or transmitted. Verify card holder address and require Card Verification Value (CVV) code to help authenticate and validate card holder information.

Monitor: Implement software code integrity checks by scanning the payment website for irregularities within the software code (JavaScript). Monitor and analyze web logs.

NOVEMBER 2, 2020

RUSSIAN CYBERCRIMINAL SENTENCED TO PRISON FOR ROLE IN $100 MILLION BOTNET CONSPIRACY

A Russian national was sentenced on October 30th to eight years in prison for his role in operating a sophisticated scheme to steal and traffic sensitive personal and financial information in the online criminal underground that resulted in an estimated loss of over $100 million.

Acting Assistant Attorney General Brian C. Rabbitt of the Justice Department's Criminal Division, U.S. Attorney G. Zachary Terwilliger for the Eastern District of Virginia, and Special Agent in Charge Matthew Miller of the U.S. Secret Service's Washington Field Office made the announcement after the sentencing by Senior U.S. District Judge T.S. Ellis III.

Aleksandr Brovko, 36, formerly of the Czech Republic, pleaded guilty in February to conspiracy to commit bank and wire fraud. According to court documents, Brovko was an active member of several elite, online forums designed for Russian-speaking cybercriminals to gather and exchange their criminal tools and services.

"This investigation is a prime example of the Secret Service's investigative mission; to protect the U.S. financial infrastructure by pursuing counterfeit and financial crimes investigations," said Special Agent in Charge Matthew Miller of the Secret Service Washington Field Office. "The Secret Service in alliance with state and local law enforcement is dedicated to effectively identifying those victimizing our communities and bringing them to justice."

"For over a decade, Brovko participated in a scheme to gain access to Americans' personal and financial information, causing more than $100 million in intended loss," said Acting Assistant Attorney General Brian C. Rabbitt of the Justice Department's Criminal Division. "This prosecution and the sentence imposed show the department's commitment to work with our international and state counterparts to bring cybercriminals to justice no matter where they are located."

"Aleksandr Brovko used his programming skills to facilitate the large-scale theft and use of stolen personal and financial information, resulting in over $100 million in intended loss," said U.S. Attorney G. Zachary Terwilliger for the Eastern District of Virginia. "Our office is committed to holding these criminals accountable and protecting our communities as cybercrime becomes an ever more prominent threat. I also want to thank our prosecutors and investigative partners for their terrific work on this complex case."

As reflected in court documents, from 2007 through 2019, Brovko worked closely with other cybercriminals to monetize vast troves of data that had been stolen by "botnets," or networks of infected computers. Brovko, in particular, wrote software scripts to parse botnet logs and performed extensive manual searches of the data in order to extract easily monetized information, such as personally identifiable information and online banking credentials. Brovko also verified the validity of stolen account credentials, and even assessed whether compromised financial accounts had enough funds to make it worthwhile to attempt to use the accounts to conduct fraudulent transactions.

According to court documents, Brovko possessed and trafficked over 200,000 unauthorized access devices during the course of the conspiracy. These access devices consisted of either personally identifying information or financial account details. Under the U.S. Sentencing Guidelines, the estimated intended loss in this case has been calculated as exceeding $100 million.

Senior Trial Attorney Laura Fong of the Criminal Division's Computer Crime and Intellectual Property Section, Assistant U.S. Attorney Alexander P. Berrang, and former Assistant U.S. Attorney Kellen Dwyer prosecuted the case. In addition, the Justice Department's Office of International Affairs and the Cybercrime Intelligence Unit of the New York County District Attorney's Office provided critical assistance. The Department of Justice also appreciates the significant cooperation and assistance provided by authorities in the Czech Republic.

SECRET SERVICE ANNOUNCES CYBER TRAINING ENHANCEMENTS

Cyber Training Unification

At the direction of the Assistant Director for the U.S. Secret Service Office of Investigations, the National Computer Forensics Institute (NCFI) in Hoover, AL and the Headquarters-based Criminal Investigative Division (CID) are unifying all cyber training through the NCFI. This structural change streamlines curriculum development and procurement of technology, maximizes usage of facility training space, and ensures consistency across various cyber investigative training disciplines.

As part of the training unification process, the NCFI and CID formalized Cyber Curriculum Development Groups, which consist of technical personnel from CID, NCFI, the Investigative Support Division, Secret Service field offices, as well as contractors and state and local Task Force Officers, who will establish the foundation for academic accreditation pursued by the NCFI. Additionally, the NCFI-Lab at the University of Tulsa, the NCFI Technical Advisory Council, and academic partners on contract with the NCFI will enhance the curriculum unification process.

Distance learning continues through the NCFI Virtual Training Platform. The NCFI anticipates holding approximately 30 classes for more than 1,000 personnel between November 2020 and February 2021. Thus far, in FY 2021, NCFI has trained more than 300 State, Local, Tribal and Territorial (SLTT) and Secret Service personnel.

In FY 2020, the NCFI trained more than 2,800 SLTT law enforcement personnel, prosecutors and judicial officials in 84 classes, both online and in person. Additionally, over 630 Secret Service personnel, as well as other federal law enforcement, received cyber training in NCFI courses.

Accreditation of Training Curriculum

There have been significant advances toward the goal of NCFI students receiving college hour credit for NCFI coursework. NCFI program managers interviewed the post-secondary regional accrediting body Cognia, and the American Council on Education (ACE), as well as reviewed the Federal Law Enforcement Training Accreditation process. ACE best aligns with the NCFI's goal, as it offers NCFI students the ability to earn course credit from over 400 colleges and universities nationwide. Current work at both the NCFI-Lab (tool testing) and the Course Competency Gap study, as well as the development of a post-training examination system, will be incorporated into satisfying ACE requirements. As an additional short-term measure, NCFI contacted individual universities regarding credit hours for NCFI students. Of those universities, progress towards the goal continues with the University of Texas at San Antonio, Marshall University, and Oklahoma State University.

Forensic Partner Reporting Program

Despite the challenges of the COVID-19 pandemic, FY 2020 was a banner year for Secret Service SLTT law enforcement partners who participated in the NCFI Forensic Partner Reporting (FPR) program.

Forensic examiners trained at the NCFI conducted digital forensic examinations in all types of criminal investigation across the nation this past year. Partners reported more than 84,600 digital forensic exams completed, and over 12.6 petabytes of data examined; an all-time record since the establishment of the FPR program in 2011!

WHAT CAN THE SECRET SERVICE TEAM AT THE NATIONAL CYBER FORENSICS AND TRAINING ALLIANCE DO FOR YOU?

The National Cyber Forensics and Training Alliance (NCFTA) is a non-profit corporation founded in 2002, focused on identifying, mitigating, and neutralizing cyber-crime threats globally. The NCFTA was created by industry and law enforcement for the sole purpose of establishing a neutral, trusted environment that enables two-way information sharing with the ultimate goal to identify, mitigate, disrupt, and neutralize cyber threats. By working across multiple industry sectors, agencies, and partnering institutions, the NCFTA is able to defeat significant domestic and global cyber threats. The NCFTA is headquartered in Pittsburgh, PA, with offices in New York, NY, and Los Angeles, CA, and currently has approximately 150 partners. The Secret Service has been a partner since 2014.

NCFTA Programs

Engagement with the NCFTA provides access to real-time reporting from industry partners, to include IOC's and related fraud trends. Additionally, the NCFTA employs a dedicated staff of analysts with access to various vendor tools and resources. There are also engagement opportunities with representatives from numerous domestic law enforcement agencies and international partners.

The NCFTA is built around three core programs:

- Cyber Financial Program (CyFin) – provides a dedicated platform for real time threat sharing within the financial industry, with a subsequent focus on mitigating such threats through various countermeasures and intelligence reports. The weekly Common Points of Purchase (CPP) Bulletin is one such report.
- Brand and Consumer Protection Program (BCP) – focuses on the use of the internet for the sale of consumer goods, including ecommerce fraud and counterfeit merchandise.
- Malware and Cyber Threats Program (MCT) – identifies, researches, and analyzes technical cyber threats, and provides alerts through data feeds and reports. The regularly updated NCFTA Ransomware Data Leaks report is one example.

These programs will be explored more fully in a future CFTF bulletin.

Requesting Assistance

Requests for assistance should be coordinated through your local Secret Service CFTF representative.

December 9, 2020

SECRET SERVICE HOSTS 3rd VIRTUAL CYBER INCIDENT RESPONSE SIMULATION

The Secret Service hosted a virtual Cyber Incident Response Simulation for financial services, real estate, retail and hospitality executives who trained on mitigation strategies for a simulated business email compromise (BEC) attack. BEC is a sophisticated scam targeting both businesses and individuals performing a transfer of funds. The scam is frequently carried out when a subject compromises legitimate business e-mail accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds.

The training was the fifth of its kind and the third virtual event hosted by the Secret Service and its Cyber Fraud Task Force (CFTF) partners. It offered executives who play an active part within their organization's cyber incident response a simulated scenario to enhance planning, collaboration and information sharing between private organizations and the Secret Service.

"The amount of information stored digitally is staggering and the potential cost of a similar attack on a large corporation could be devastating," said U.S. Secret Service Director Jim Murray to participants of the exercise. "Our ability to effectively respond to cyber incidents, like the one we are modeling in our exercise today, is tied very closely to the strength of our relationships with businesses and organizations just like yours."

As the cyber mission of the Secret Service expands, the agency has adopted a multifaceted approach inclusive of education and information sharing, as well as the enhanced development of partnerships with industry representatives. Event participants worked through a uniquely designed cybercrime crisis role-play simulation in order to gain experience, knowledge, and a better understanding of how to efficiently and effectively respond to a BEC attack.

"Cyber incident response simulations are critical to ensuring we have the skills, technology, infrastructure, and public-private sector relationships to respond should a cyber incident occur," said Secretary of the Treasury Steven T. Mnuchin who joined Director Murray at Secret Service Headquarters. "Treasury continues to work with our interagency, international, and industry partners to strengthen our defenses against malicious cyber incidents, as well as ensure swift response efforts to recover related financial losses."

The event featured guest speakers from across law enforcement as well as industry executives who discussed a range of topics including:

- partnerships between the Secret Service, the Department of Homeland Security Cyber Infrastructure Security Agency (CISA); Mastercard, Hogan Lovells and FinCEN;
- the complex cyber-threat environment;
- the needs of organizations victimized by cybercrime, and;

- the capabilities, investigative processes and tools of the Secret Service, specifically the capabilities of the CFTF partners.

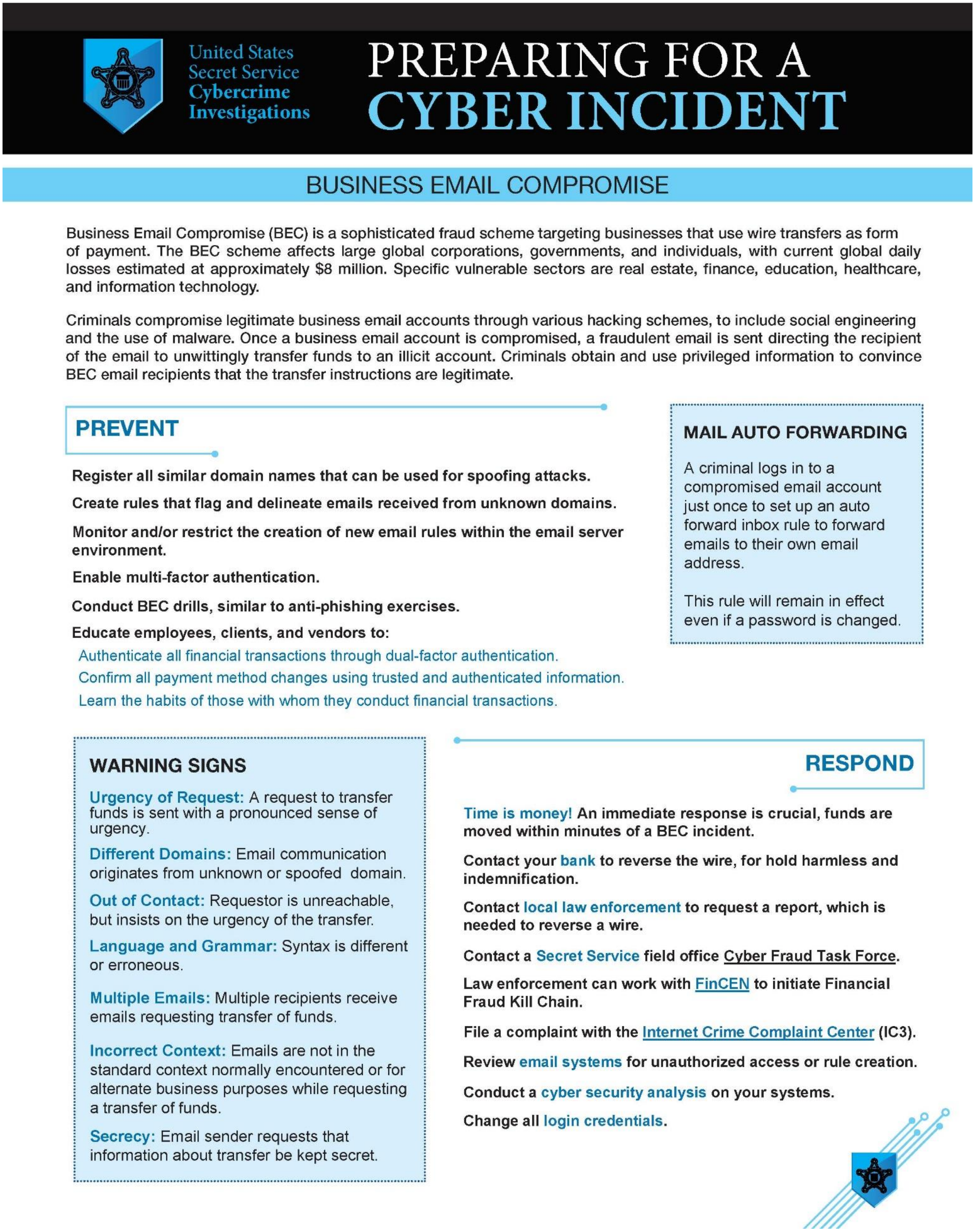
The following resource was provided to those who attended by one of our panelists, Peter Marta of Hogan Lovells. The white paper addresses legal resources on best practices in this area. Mr. Marta authored this article that was also published online in Bloomberg Law last year. The link to the article is:

https://www.engage.hoganlovells.com/knowledgeservices/news/lessons-for-in-house-counsel-from-cybersecuritys-front-lines

In addition, the following page offers some further information on BEC prevention, warning signs, and response.

The Secret Service will host its next Cyber Incident Response Simulation in early February 2021. Additional information on this event can be obtained through your local CFTF.

SECRET SERVICE PUBLISHES BEC GUIDE



United States
Secret Service
Cybercrime
Investigations

PREPARING FOR A CYBER INCIDENT

BUSINESS EMAIL COMPROMISE

Business Email Compromise (BEC) is a sophisticated fraud scheme targeting businesses that use wire transfers as form of payment. The BEC scheme affects large global corporations, governments, and individuals, with current global daily losses estimated at approximately $8 million. Specific vulnerable sectors are real estate, finance, education, healthcare, and information technology.

Criminals compromise legitimate business email accounts through various hacking schemes, to include social engineering and the use of malware. Once a business email account is compromised, a fraudulent email is sent directing the recipient of the email to unwittingly transfer funds to an illicit account. Criminals obtain and use privileged information to convince BEC email recipients that the transfer instructions are legitimate.

PREVENT

Register all similar domain names that can be used for spoofing attacks.

Create rules that flag and delineate emails received from unknown domains.

Monitor and/or restrict the creation of new email rules within the email server environment.

Enable multi-factor authentication.

Conduct BEC drills, similar to anti-phishing exercises.

Educate employees, clients, and vendors to:

Authenticate all financial transactions through dual-factor authentication.

Confirm all payment method changes using trusted and authenticated information.

Learn the habits of those with whom they conduct financial transactions.

MAIL AUTO FORWARDING

A criminal logs in to a compromised email account just once to set up an auto forward inbox rule to forward emails to their own email address.

This rule will remain in effect even if a password is changed.

WARNING SIGNS

Urgency of Request: A request to transfer funds is sent with a pronounced sense of urgency.

Different Domains: Email communication originates from unknown or spoofed domain.

Out of Contact: Requestor is unreachable, but insists on the urgency of the transfer.

Language and Grammar: Syntax is different or erroneous.

Multiple Emails: Multiple recipients receive emails requesting transfer of funds.

Incorrect Context: Emails are not in the standard context normally encountered or for alternate business purposes while requesting a transfer of funds.

Secrecy: Email sender requests that information about transfer be kept secret.

RESPOND

Time is money! An immediate response is crucial, funds are moved within minutes of a BEC incident.

Contact your bank to reverse the wire, for hold harmless and indemnification.

Contact local law enforcement to request a report, which is needed to reverse a wire.

Contact a Secret Service field office Cyber Fraud Task Force.

Law enforcement can work with FinCEN to initiate Financial Fraud Kill Chain.

File a complaint with the Internet Crime Complaint Center (IC3).

Review email systems for unauthorized access or rule creation.

Conduct a cyber security analysis on your systems.

Change all login credentials.

LEGAL & POLICY DEVELOPMENTS

U.S. DEPARTMENT OF THE TREASURY’S OFFICE OF FOREIGN ASSETS CONTROL ISSUES RANSOMWARE ADVISORY ON POTENTIAL SANCTIONS RISKS

The U.S. Department of the Treasury’s Office of Foreign Assets Control (OFAC) is issuing an advisory to alert companies that engage with victims of ransomware attacks of the potential sanctions risks for facilitating ransomware payments. This advisory highlights OFAC’s designations of malicious cyber actors and those who facilitate ransomware transactions under its cyber-related sanctions program. It identifies U.S. government resources for reporting ransomware attacks and provides information on the factors OFAC generally considers when determining an appropriate enforcement response to an apparent violation, such as the existence, nature, and adequacy of a sanctions compliance program. ***The advisory also encourages financial institutions and other companies that engage with victims of ransomware attacks to report such attacks to and fully cooperate with law enforcement, as these will be considered significant mitigating factors.***

The full version of the advisory can be found on the U.S. Department of the Treasury’s website in the Office of Foreign Assets Control section or via the link provided below:

https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf

FinCEN ADVISORY ON RANSOMWARE AND THE USE OF THE FINANCIAL SYSTEM TO FACILITATE RANSOM PAYMENTS

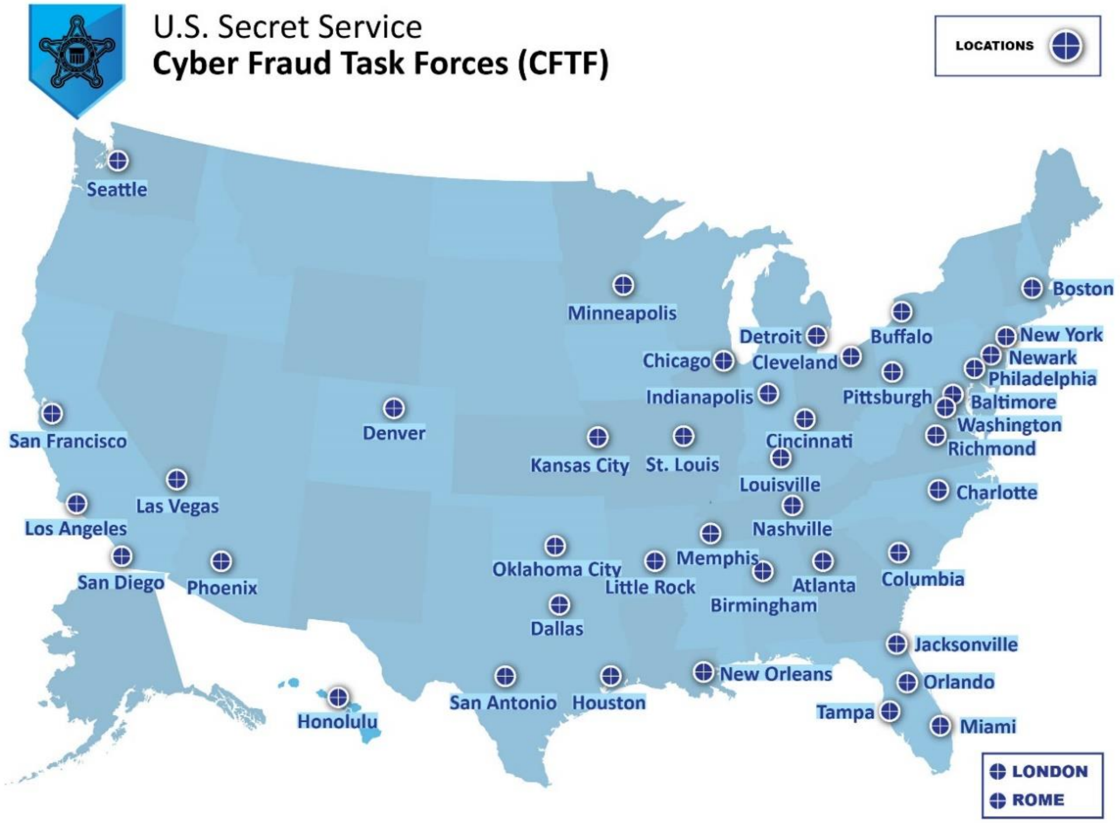
In conjunction with the OFAC advisory above, the U.S. Department of Treasury’s Financial Crimes Enforcement Network (FinCEN) issued an advisory, entitled “Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments.” This advisory provides information on the role of financial intermediaries in payments, ransomware trends and typologies, and related financial red flags. It also provides information on effectively reporting and sharing information related to ransomware attacks.

The full version of the advisory can be found on the FinCEN website in the Advisories section, on the U.S. Department of the Treasury’s website in the Press Releases section, or via the link provided below:

https://www.fincen.gov/sites/default/files/advisory/2020-10-01/Advisory%20Ransomware%20FINAL%20508.pdf

CFTF LOCATIONS

Atlanta, GA	404-331-6111
Baltimore, MD	443-263-1100
Birmingham, AL	205-731-1144
Boston, MA	617-565-5640
Buffalo, NY	716-551-4401
Charlotte, NC	704-442-8370
Chicago, IL	312-353-5431
Cincinnati, OH	513-684-3585
Cleveland, OH	216-750-2058
Columbia, SC	803-772-4015
Dallas, TX	972-868-3200
Denver, CO	303-850-2700
Detroit, MI	313-226-6400
Honolulu, HI	808-541-1912
Houston, TX	713-868-2299
Indianapolis, IN	317-635-6420
Jacksonville, FL	904-296-0133
Kansas City, MO	816-460-0600
Las Vegas, NV	702-868-3000
Little Rock, AR	501-324-6241
Los Angeles, CA	213-894-4830
Louisville, KY	502-582-5171
Memphis, TN	901-544-0333
Miami, FL	305-863-5000
Minneapolis, MN	612-348-1800
Nashville, TN	615-736-5841
Newark, NJ	973-971-3100
New Orleans, LA	504-841-3260
New York, NY	718-840-1000
Oklahoma City, OK	405-272-0630
Orlando, FL	407-648-6333
Philadelphia, PA	215-861-3300
Phoenix, AZ	602-640-5580
Pittsburgh, PA	412-281-7825
Richmond, VA	804-592-3086
San Antonio, TX	210-308-6220
San Diego, CA	619-557-5640
San Francisco, CA	415-576-1210
Seattle, WA	206-553-1922
St. Louis, MO	314-539-2238
Tampa, FL	813-228-2636
Washington, DC	202-406-8800
London, England	
Rome, Italy	


U.S. Secret Service
Cyber Fraud Task Forces (CFTF)