Hot Topics in Cybersecurity Explained

Hosted by the IP and Information Law Affinity Group

Join Fordham Law School alumnus and fellow practitioners as they discuss current issues on cybersecurity trends, the burst of enforcement activity in cyber, and best practices on how companies can avoid hacks (and government attention).

Wednesday, December 8, 2021
5:30 - 7:00 p.m. EST
COURSE MATERIALS
CLE Materials: Table of Contents

1. Speaker Biographies
   a. Panelists
      a. Sean Farrell '07, Chief, Cybercrime Unit, U.S. Attorney's Office, District of New Jersey
      b. Kelly Ann Harris, Director & Asst. General Counsel, Cybersecurity, Incident Response & Privacy, Deloitte
      c. Jamie Yavelberg, Director, Fraud Section, USDOJ Commercial Litigation Branch
      d. Haseen Usman Ahmed, Chief Information Security Officer, CohereCyberSecure
   b. Moderator
      a. David Feder '07, Counsel, Fenwick & West LLP

2. CLE Materials
   a. 2020 Internet Crime Report
   b. Announcement of National Cryptocurrency Enforcement Team
   c. Announcement of New Civil Cyber-Fraud Initiative
   d. Executive Order on Improving the Nation's Cybersecurity
   e. FBI Press Release - FBI Strategy Addresses Evolving Cyber Threat
   f. FinCEN BitMEX announcement
   g. FTC Announcement GLB Safeguards Rule
   h. Guo Wengui v Clark Hill PLC
   i. In re Capital One Consumer Data Security Breach Litigation
   j. In re Rutters Data Security Breach Litigation
   k. NYDFS ISSUES REPORT ON THE SOLARWINDS SUPPLY CHAIN ATTACK
   l. NYDFS Microsoft Reports Exploitation of Four Vulnerabilities in Microsoft Exchange Server
   m. Advisory on Potential Sanctions Risks for Facilitation Ransomware Payments
   n. United States v Aerojet Rocketdyne Holdings Inc.
Speaker Bios

Sean Farrell ’07
Chief, Cybercrime Unit, U.S. Attorney’s Office, District of New Jersey
Sean Farrell currently serves as the Chief of the Cybercrime Unit in the U.S. Attorney’s Office for the District of New Jersey. While in the U.S. Attorney’s Office, Sean also worked as an AUSA in the Special Prosecutions Division, where he handled public corruption matters. Before joining the U.S. Attorney’s Office, he worked as a Trial Attorney and, later, as an Assistant Chief, in the U.S. Department of Justice’s Antitrust Division. Prior to joining the Department of Justice, Sean was a litigation associate at Milbank LLP and clerked for the Hon. Arthur D. Spatt in the Eastern District of New York. Sean graduated with honors from both Fordham University School of Law and Binghamton University.

David Feder ’07
Counsel, Fenwick & West LLP
David represents technology and life sciences companies in a broad range of complex commercial litigation matters, with a focus on privacy and cybersecurity litigation, counseling and investigations. Before joining Fenwick, David spent nearly a decade at the U.S. Attorney’s Office for the District of New Jersey, most recently as Chief of the Cybercrime Unit. In this role, he managed a team of Assistant U.S. Attorneys focused on the investigation and prosecution of computer network intrusions, computer-enabled fraud, intellectual property offenses and international money laundering. David personally litigated and supervised hundreds of cybercrime matters, including ransomware and digital extortion, payment card and PII theft, botnets, digital currency fraud, hack-to-trade securities fraud, dark market sites and vendors, unlicensed money transmitters and business email compromise. He also worked closely with key cyberlaw enforcement partners, including the Computer Crime and Intellectual Property Section of the Department of Justice, FBI, U.S. Secret Service, DHS and IRS, and the cyber components of regulatory authorities, including the SEC, CFTC and FinCEN. As an AUSA, David handled numerous jury trials, hearings and appellate arguments, involving securities and commodities fraud, credit card and other commercial frauds, and public corruption, among others. He received an Attorney General’s Award for his role in securing the largest-ever civil settlement obtained by the DOJ on FIRREA claims relating to residential mortgage-backed securities practices. David secured precedential opinions after arguing before the Third Circuit on the standards for sophisticated money laundering and the elements of wire fraud. He conducted parallel investigations into investment fraud, FCPA violations, digital currency fraud and Ponzi schemes with the SEC and CFTC. David also served as the Office’s coordinator for Discovery and Electronic Evidence and presented regularly on cybercrime and digital evidence issues.

Kelly Ann Harris
Director & Asst. General Counsel, Cybersecurity, Incident Response & Privacy, Deloitte
Kelly Harris currently serves as Assistant General Counsel for Cybersecurity, Privacy and Incident Response at Deloitte Global. Before joining Deloitte, she spent 11 years building privacy and information security programs at Prudential Financial and Wyndham Worldwide. She started her legal career as an associate with Kirkpatrick & Lockhart (now K&L Gates) and then Gibbons P.C. before going in-house to Japanese pharmaceutical companies Daiichi Sankyo and Otsuka.

Haseen Usman Ahmed
Chief Information Security Officer, CohereCyberSecure
Haseen Usman Ahmed is the Chief Information Security Officer (CISO) at Cohere Cyber Secure. Previously the Head of IT Security, Global PCI-IS Standards Compliance & Cyber Defense Center at Habib Bank Limited, Mr. Usman has a significant amount of expertise in the various domains of information security. With over 18 years of professional experience in advanced cybersecurity disciplines within different industries, Haseen holds multiple certifications in advanced malware analysis, digital forensics, malware program testing, incident handling and response,
compliance testing, and cyber threat intelligence defense. Mr. Usman directly oversaw IT Security, payment systems security, and IS standards compliances in PCI DSS, ISO 27001, GDPR, PA DSS, NIST, 3DSecure, and other security-related operations for 23 million+ worldwide customers. Mr. Usman is an active participant for international principal security bodies that are engaged in different developmental cyber security training and certifications for NATO, NASA, Boeing Aerospace, US Military, US Air force, and various federal and governmental operations entities. As an active speaker, Haseen has conducted conferences and also trained thousands of security professionals globally across different disciplines and is also an authorized principal auditor. Haseen is the author of a book on payment system security and contributor for IS Security standards for 25+ global IS certifications.

Jamie Yavelberg
Director, Fraud Section, USDOJ Commercial Litigation Branch

Jamie Yavelberg works in the Civil Division of the United States Department of Justice. She leads the Department’s enforcement of the False Claims Act and FIRREA as the Director of the Fraud Section in the Commercial Litigation Branch. Over the course of her career, she has handled a wide range of civil matters, including those involving health care providers, pharmaceutical and device companies, government contractors, and financial institutions.
INTERNET CRIME REPORT
2020
# 2020 Internet Crime Report

## TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>3</td>
</tr>
<tr>
<td>About the Internet Crime Complaint Center</td>
<td>4</td>
</tr>
<tr>
<td>IC3 History</td>
<td>5</td>
</tr>
<tr>
<td>The IC3 Role in Combating Cyber Crime</td>
<td>7</td>
</tr>
<tr>
<td>IC3 Core Functions</td>
<td>8</td>
</tr>
<tr>
<td>Hot Topics for 2020</td>
<td>9</td>
</tr>
<tr>
<td>Business Email Compromise (BEC)</td>
<td>10</td>
</tr>
<tr>
<td>IC3 Recovery Asset Team (RAT)</td>
<td>11</td>
</tr>
<tr>
<td>RAT Successes</td>
<td>12</td>
</tr>
<tr>
<td>Tech Support Fraud</td>
<td>13</td>
</tr>
<tr>
<td>Ransomware</td>
<td>14</td>
</tr>
<tr>
<td>2020 Victims by Age Group</td>
<td>16</td>
</tr>
<tr>
<td>2020 - Top 20 International Victim Countries</td>
<td>17</td>
</tr>
<tr>
<td>2020 - Top 10 States by Number of Victims</td>
<td>18</td>
</tr>
<tr>
<td>2020 - Top 10 States by Victim Loss</td>
<td>18</td>
</tr>
<tr>
<td>2020 Crime Types</td>
<td>19</td>
</tr>
<tr>
<td>Last 3 Year Complaint Count Comparison</td>
<td>21</td>
</tr>
<tr>
<td>2020 Overall State Statistics</td>
<td>23</td>
</tr>
<tr>
<td>Appendix A: Definitions</td>
<td>27</td>
</tr>
<tr>
<td>Appendix B: Additional information about IC3 Data</td>
<td>30</td>
</tr>
</tbody>
</table>
INTRODUCTION

Dear Reader,

In 2020, while the American public was focused on protecting our families from a global pandemic and helping others in need, cyber criminals took advantage of an opportunity to profit from our dependence on technology to go on an Internet crime spree. These criminals used phishing, spoofing, extortion, and various types of Internet-enabled fraud to target the most vulnerable in our society - medical workers searching for personal protective equipment, families looking for information about stimulus checks to help pay bills, and many others.

Crimes of this type are just a small part of what the FBI combats through our criminal and cyber investigative work. Key to our cyber mission is the Internet Crime Complaint Center (IC3), which provides the public with a trustworthy source for information on cyber criminal activity, and a way for the public to report directly to us when they suspect they are a victim of cyber crime.

IC3 received a record number of complaints from the American public in 2020: 791,790, with reported losses exceeding $4.1 billion. This represents a 69% increase in total complaints from 2019. Business E-mail Compromise (BEC) schemes continued to be the costliest: 19,369 complaints with an adjusted loss of approximately $1.8 billion. Phishing scams were also prominent: 241,342 complaints, with adjusted losses of over $54 million. The number of ransomware incidents also continues to rise, with 2,474 incidents reported in 2020.

Public reporting is central to the mission and success of IC3. Submitting a cyber crime complaint to IC3.gov not only helps the FBI address specific complaints—and provide support and assistance to victims—but also helps us prevent additional crimes by finding and holding criminal actors accountable. Information reported to the IC3 helps the FBI better understand the motives of cyber-criminals, the evolving threat posed, and tactics utilized, enabling us to most effectively work with partners to mitigate the damage to victims.

IC3 has continued to strengthen its relationships with industry and others in the law enforcement community to reduce financial losses resulting from BEC scams. Through the Recovery Asset Team, IC3 worked with its partners to successfully freeze approximately $380 million of the $462 million in reported losses in 2020, representing a success rate of nearly 82%. In addition, IC3 has a Recovery and Investigative Development Team which assists financial and law enforcement investigators in dismantling organizations that move and transfer funds obtained illicitly.

With our dedicated resources focused on recovering funds and preventing further victimization, we are better aligned to confront the unique challenges faced in cyberspace. Visit IC3.gov to access the latest information on criminal Internet activity.

We strongly encourage readers to submit complaints to IC3 and to reach out to their local FBI field office to report malicious cyber criminal activity. Together we will continue to build safety, security, and confidence in our digitally connected world.

Paul Abbate
Deputy Director
Federal Bureau of Investigation
ABOUT THE INTERNET CRIME COMPLAINT CENTER

The mission of the FBI is to protect the American people and uphold the Constitution of the United States. The mission of the IC3 is to provide the public with a reliable and convenient reporting mechanism to submit information to the FBI concerning suspected Internet-facilitated criminal activity, and to develop effective alliances with industry partners. Information is analyzed and disseminated for investigative and intelligence purposes for law enforcement, and for public awareness.

To promote public awareness, the IC3 produces this annual report to aggregate and highlight the data provided by the general public. The quality of the data is directly attributable to the information ingested via the public interface, www.ic3.gov. The IC3 attempts to standardize the data by categorizing each complaint based on the information provided. The IC3 staff analyzes the data to identify trends in Internet-facilitated crimes and what those trends may represent in the coming year.

As a response to the increasing prevalence of fraud against the elderly, the Department of Justice and the FBI partnered to create the Elder Justice Initiative. Elder Fraud is defined as a financial fraud scheme which targets or disproportionately affects people over the age of 60. The FBI, including IC3, has worked tirelessly to educate this population on how to take steps to protect themselves from being victimized.

In 2020, the IC3 received 105,301 complaints from victims over the age of 60 with total losses in excess of $966 million. Since, age is not a required reporting field, these statistics only reflect complaints in which the victim voluntarily provided their age range as “OVER 60.” Victims over the age of 60 are targeted by perpetrators because they are believed to have significant financial resources.

Victims over the age of 60 may encounter scams including Advance Fee Schemes, Investment Fraud Schemes, Romance Scams, Tech Support Scams, Grandparent Scams, Government Impersonation Scams, Sweepstakes/Charity/Lottery Scams, Home Repair Scams, TV/Radio Scams, and Family/Caregiver Scams. If the perpetrators are successful after initial contact, they will often continue to victimize these individuals. Further information about the Elder Justice Initiative is available at https://www.justice.gov/elderjustice.

As a result of the significant increases and impact of scams targeting the elderly, IC3 is planning to release its first annual report focusing entirely on Elder Fraud in 2021.
IC3 History
In May 2000, the IC3 was established as a center to receive complaints of Internet crime. A total of 5,679,259 complaints have been reported to the IC3 since its inception. Over the last five years, the IC3 has received an average of 440,000 complaints per year. These complaints address a wide array of Internet scams affecting victims across the globe.1

IC3 Complaint Statistics
Last Five Years

2,211,396 TOTAL COMPLAINTS

$13.3 Billion TOTAL LOSSES*
(Rounded to the nearest million)

1 Accessibility description: Image includes yearly and aggregate data for complaints and losses over the years 2016 to 2020. Over that time, IC3 received a total of 2,211,396 complaints, reporting a loss of $13.3 billion.
IC3 Complaint Statistics
2020 - Top 5 Crime Type Comparison
Last Five Years

Accessibility description: Image includes a victim loss comparison for the top five reported crime types of 2020 for the years of 2016 to 2020.
The IC3 Role in Combating Cyber Crime

WHAT WE DO

- Host a Portal where Victims Report Internet Crime at www.ic3.gov
- Provide a Central Hub to Alert the Public
- Partner with Private Sector and with Local, State, Federal, and International Agencies
- Host a Remote Access Database for all Law Enforcement via the FBI’s LEEP website
- Perform Analysis, Complaint Referrals, and Asset Recovery

Accessibility description: Image lists IC3’s primary functions including providing a central hub to alert the public to threats; hosting a victim reporting portal at www.ic3.gov; partnering with private sector and with local, state, federal, and international agencies; increasing victim reporting via outreach; and hosting a remote access database for all law enforcement via the FBI’s LEEP website.
## IC3 Core Functions

<table>
<thead>
<tr>
<th>COLLECTION</th>
<th>ANALYSIS</th>
<th>PUBLIC AWARENESS</th>
<th>REFERRALS</th>
</tr>
</thead>
<tbody>
<tr>
<td>The IC3 is the central point for Internet crime victims to report and alert the appropriate agencies to suspected criminal Internet activity. Victims are encouraged and often directed by law enforcement to file a complaint online at <a href="http://www.ic3.gov">www.ic3.gov</a>. Complainants are asked to document accurate and complete information related to Internet crime, as well as any other relevant information necessary to support the complaint.</td>
<td>The IC3 reviews and analyzes data submitted through its website to identify emerging threats and new trends.</td>
<td>Public service announcements, industry alerts, and other publications outlining specific scams are posted to the <a href="http://www.ic3.gov">www.ic3.gov</a> website. As more people become aware of Internet crimes and the methods used to carry them out, potential victims are equipped with a broader understanding of the dangers associated with Internet activity and are in a better position to avoid falling prey to schemes online.</td>
<td>The IC3 aggregates related complaints to build referrals, which are forwarded to local, state, federal, and international law enforcement agencies for potential investigation. If law enforcement conducts an investigation and determines a crime has been committed, legal action may be brought against the perpetrator.</td>
</tr>
</tbody>
</table>

---

4 Accessibility description: Image contains icons with the core functions. Core functions - Collection, Analysis, Public Awareness, and Referrals - are listed in individual blocks as components of an ongoing process.
HOT TOPICS FOR 2020
COVID-19

The year 2020 will forever be remembered as the year of the COVID-19 pandemic. The global impact was unlike anything seen in recent history, and the virus permeated all aspects of life. Fraudsters took the opportunity to exploit the pandemic to target both business and individuals. In 2020, the IC3 received over 28,500 complaints related to COVID-19.

Fraudsters targeted the Coronavirus Aid, Relief, and Economic Security Act (CARES Act), which included provisions to help small businesses during the pandemic. The IC3 received thousands of complaints reporting emerging financial crime revolving around CARES Act stimulus funds, specifically targeting unemployment insurance, Paycheck Protection Program (PPP) loans, and Small Business Economic Injury Disaster Loans, as well as other COVID-related fraud.

Most of the IC3 complaints related to CARES Act fraud involved grant fraud, loan fraud, and phishing for Personally Identifiable Information (PII). Complaints have been filed from citizens in several states describing fraudulently submitted online unemployment insurance claims using their identities. Many victims of this identity theft scheme did not know they had been targeted until they attempted to file their own legitimate claim for unemployment insurance benefits. At that time, they received a notification from the state unemployment insurance agency, received an IRS Form 1099-G showing the benefits collected from unemployment insurance, or were notified by their employer that a claim had been filed while the victim is still employed.

People are encouraged to protect themselves from scammers by:

- Using extreme caution in online communication. Verify the sender of an email. Criminals will sometimes change just one letter in an email address to make it look like one you know. Also, be very wary of attachments or links. Hover your mouse over a link before clicking to see where it is sending you.
- Questioning anyone offering you something that is “too good to be true” or is a secret investment opportunity or medical advice.
- Relying on trusted sources, like your own doctor, the Center for Disease Control, and your local health department for medical information and agencies like the Federal Trade Commission and Internal Revenue Service for financial and tax information.

“Unfortunately, criminals are very opportunistic. They see a vulnerable population out there that they can prey upon.” FBI Section Chief Steven Merrill, Financial Crimes Section.

One of the most prevalent schemes seen during the pandemic has been government impersonators. Criminals are reaching out to people through social media, emails, or phone calls pretending to be from the government. The scammers attempt to gather personal information or illicit money through charades or threats.

As the response to COVID-19 turned to vaccinations, scams emerged asking people to pay out of pocket to receive the vaccine, put their names on a vaccine waiting, or obtain early access. Fraudulent advertisements for vaccines popped up on social media platforms, or came via email, telephone calls, online, or from unsolicited/unknown sources.

As we continue to battle COVID-19, protect yourself from fraud and scams. Do not give out your personal information to unknown sources. If you are a victim of an online crime involving COVID-19, report it.
Business Email Compromise (BEC)

In 2020, the IC3 received 19,369 Business Email Compromise (BEC)/Email Account Compromise (EAC) complaints with adjusted losses of over $1.8 billion. BEC/EAC is a sophisticated scam targeting both businesses and individuals performing transfers of funds. The scam is frequently carried out when a subject compromises legitimate business email accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds.

As the fraudsters have become more sophisticated, the BEC/EAC scheme has evolved in kind. In 2013, BEC/EAC scams routinely began with the hacking or spoofing of the email accounts of chief executive officers or chief financial officers, and fraudulent emails were sent requesting wire payments be sent to fraudulent locations. Over the years, the scam evolved to include compromise of personal emails, compromise of vendor emails, spoofed lawyer email accounts, requests for W-2 information, the targeting of the real estate sector, and fraudulent requests for large amounts of gift cards.

In 2020, the IC3 observed an increase in the number of BEC/EAC complaints related to the use of identity theft and funds being converted to cryptocurrency. In these variations, we saw an initial victim being scammed in non-BEC/EAC situations to include Extortion, Tech Support, Romance scams, etc., that involved a victim providing a form of ID to a bad actor. That identifying information was then used to establish a bank account to receive stolen BEC/EAC funds and then transferred to a cryptocurrency account.
IC3 RECOVERY ASSET TEAM

The Internet Crime Complaint Center’s Recovery Asset Team (RAT) was established in February 2018 to streamline communication with financial institutions and assist FBI field offices with the freezing of funds for victims who made transfers to domestic accounts under fraudulent pretenses.

RAT Process

*If criteria is met, transaction details are forwarded to the identified point of contact at the recipient bank to notify of fraudulent activity and request freezing of the account. Once response is received from the recipient bank, RAT contacts the appropriate FBI field office(s).

The RAT functions as a liaison between law enforcement and financial institutions supporting statistical and investigative analysis.

Success in 2020

Incidents: 1,303
Losses: $462,967,963.72
Frozen: $380,211,432.04
Success Rate: 82%

Goals of RAT-Financial Institution Partnership

- Assist in the identification of potentially fraudulent accounts across the sector.
- Remain at the forefront of emerging trends among financial fraud schemes.
- Foster a symbiotic relationship in which information is appropriately shared.

Guidance for BEC Victims

- Contact the originating financial institution as soon as fraud is recognized to request a recall or reversal and a Hold Harmless Letter or Letter of Indemnity.
- File a detailed complaint with www.ic3.gov. It is vital the complaint contain all required data in provided fields, including banking information.
- Visit www.ic3.gov for updated PSAs regarding BEC trends as well as other fraud schemes targeting specific populations, like trends targeting real estate, pre-paid cards, and W-2s, for example.
- Never make any payment changes without verifying the change with the intended recipient; Verify email addresses are accurate when checking email on a cell phone or other mobile device.

Accessibility description: Image shows the different stages of a complaint in the RAT process.
RAT Successes

The IC3 RAT has proven to be a valuable resource for field offices and victims. The following are three examples of the RAT’s successful contributions to investigative and recovery efforts.

St. Louis

In June 2020, the IC3 received a complaint filed by a victim company regarding a wire transfer of $60 million to a fraudulent overseas bank account in Hong Kong. The reported transaction date fell outside of the International Financial Fraud Kill Chain (FFKC) time frame for action; however, The IC3 RAT notified the Legal Attaché of Hong Kong and the St. Louis Field Office of the large dollar loss. Through the collaboration efforts of the IC3 RAT, the Legal Attaché of Hong Kong, and Hong Kong banking and law enforcement partners, the wire was located and immediately blocked from entering the beneficiary account in Hong Kong. The St. Louis Field Office quickly contacted the victim of this incident to initiate a recall letter with the originating bank and Hong Kong Police. Through these efforts, the full amount of $60 million was returned to the victim.

Chicago

In June 2020, the IC3 was notified of two fraudulent wires totaling $977,411 sent by a victim company specializing in hand sanitizer. The money was intended for an investment in ventilators due to the COVID-19 pandemic. Upon receipt of this notification, the RAT initiated the domestic FFKC to request the recipient financial institution freeze the associated account and any remaining funds. Collaboration with the beneficiary bank resulted in the more recent of the two transfers being frozen in full. The older transfer had already been depleted via wire to a cryptocurrency exchange at another financial institution. Collaboration with the bank, which housed the cryptocurrency account, and with the cryptocurrency account holder company resulted in tracing the wallet path of the funds upon being converted into Bitcoin.

Houston

In April 2020, the IC3 received a complaint from a health care victim regarding five wire transfers totaling more than $2 million. The RAT Team initiated the FFKC and, after collaboration with the financial institution, holds were placed on the funds to allow the victim time for the indemnification process. Later inquiries into the recipient account number by the IC3 RaID Team found additional suspicious activity information from financial databases on the possible money mules involved with the account. This information was then compiled into two targeting packages and forwarded to the Houston Field Office for case enhancement purposes.
Tech Support Fraud

Tech Support Fraud continues to be a growing problem. This scheme involves a criminal claiming to provide customer, security, or technical support or service to defraud unwitting individuals. Criminals may pose as support or service representatives offering to resolve such issues as a compromised email or bank account, a virus on a computer, or a software license renewal. Recent complaints involve criminals posing as customer support for financial institutions, utility companies, or virtual currency exchanges. Many victims report being directed to make wire transfers to overseas accounts or purchase large amounts of prepaid cards.

Although pandemic lockdowns caused a brief slowdown to this fraud activity, victims still reported increases in incidences and losses to tech support fraud.

In 2020, the IC3 received 15,421 complaints related to Tech Support Fraud from victims in 60 countries. The losses amounted to over $146 million, which represents a 171 percent increase in losses from 2019.

The majority of victims, at least 66 percent, report to be over 60 years of age, and experience at least 84 percent of the losses (over $116 million).

Additional information, explanations, and suggestions for protection regarding Tech Support Fraud is available in the most recent Tech Support Fraud PSA on the IC3 website: https://www.ic3.gov/media/2018/180328.aspx.

Investigative efforts have yielded many successes, including the two examples below.

**Knoxville**

In 2016, the IC3 identified a subject receiving and processing payments for a call center conducting tech support fraud out of India. The subject received checks from victims who believed they were paying for legitimate tech support services. The subsequent investigation by the Knoxville Field Office revealed a larger group of U.S.-based subjects working with the call center owner and connected over 15,000 victims with losses of approximately $7 million. In November 2019, five subjects were indicted in U.S. District Court, Eastern District of Tennessee. By early 2020, all subjects were arrested and charged. One subject from India is accused of being the owner/director of the call center in India. Three subjects in Iowa and one subject in Maryland are accused of facilitating payments on behalf of the Indian call center. Trials are pending.

**Legat New Delhi**

In July 2018, the IC3 received a complaint filed by an Indian citizen regarding an illegal call center in Noida, India. IC3 research and analysis identified companies operating on behalf of the call center and over 130 victims who experienced losses of more than $50,000. The IC3 complaints and analysis were provided to FBI Legat New Delhi, who worked with Indian law enforcement who raided the call center in late 2018. In February 2020, confirmation was received from India’s Central Bureau of Investigation that charges were filed in India on four subjects, three of which have been arrested and incarcerated.
Ransomware

In 2020, the IC3 received 2,474 complaints identified as ransomware with adjusted losses of over $29.1 million. Ransomware is a type of malicious software, or malware, that encrypts data on a computer making it unusable. A malicious cyber criminal holds the data hostage until the ransom is paid. If the ransom is not paid, the victim’s data remains unavailable. Cyber criminals may also pressure victims to pay the ransom by threatening to destroy the victim’s data or to release it to the public.

Although cyber criminals use a variety of techniques to infect victims with ransomware, the most common means of infection are:

- Email phishing campaigns: The cyber criminal sends an email containing a malicious file or link which deploys malware when clicked by a recipient. Cyber criminals historically have used generic, broad-based spamming strategies to deploy their malware, through recent ransomware campaigns have been more targeted and sophisticated. Criminals may also compromise a victim’s email account by using precursor malware, which enables the cyber criminal to use a victim’s email account to further spread the infection.

- Remote Desktop Protocol (RDP) vulnerabilities: RDP is a proprietary network protocol that allows individuals to control the resources and data of a computer over the internet. Cyber criminals have used both brute-force methods, a technique using trial-and-error to obtain user credentials, and credentials purchased on dark web marketplaces to gain unauthorized RDP access to victim systems. Once they have RDP access, criminals can deploy a range of malware – including ransomware – to victim systems.

- Software vulnerabilities: Cyber criminals can take advantage of security weaknesses in widely used software programs to gain control of victim systems and deploy ransomware.

The FBI does not encourage paying a ransom to criminal actors. Paying a ransom may embolden adversaries to target additional organizations, encourage other criminal actors to engage in the distribution of ransomware, and /or fund illicit activities. Paying the ransom also does not guarantee that a victim’s files will be recovered. Regardless of whether you or your organization have decided to pay the ransom, the FBI urges you to report ransomware incidents to your local field office or the FBI’s Internet Crime Complaint Center (IC3). Doing so provides investigators with the critical information they need to track ransomware attackers, hold them accountable under U.S. law, and prevent future attacks.
Accessibility description: Image depicts key statistics regarding complaints and victim loss. Total losses of $4.2 billion were reported in 2020. The total number of complaints received since the year 2000 is 5,679,259. IC3 has received approximately 440,000 complaints per year on average over the last five years, or more than 2,000 complaints per day.
## 2020 Victims by Age Group

<table>
<thead>
<tr>
<th>Age Range</th>
<th>Total Count</th>
<th>Total Loss</th>
</tr>
</thead>
<tbody>
<tr>
<td>Under 20</td>
<td>23,186</td>
<td>$70,980,763</td>
</tr>
<tr>
<td>20 - 29</td>
<td>70,791</td>
<td>$197,402,240</td>
</tr>
<tr>
<td>30 - 39</td>
<td>88,364</td>
<td>$492,176,845</td>
</tr>
<tr>
<td>40 - 49</td>
<td>91,568</td>
<td>$717,161,726</td>
</tr>
<tr>
<td>50 - 59</td>
<td>85,967</td>
<td>$847,948,101</td>
</tr>
<tr>
<td>Over 60</td>
<td>105,301</td>
<td>$966,062,236</td>
</tr>
</tbody>
</table>

7 Not all complaints include an associated age range—those without this information are excluded from this table. Please see Appendix B for more information regarding IC3 data.
2020 - TOP 20 INTERNATIONAL VICTIM COUNTRIES

Excluding the United States

<table>
<thead>
<tr>
<th>Rank</th>
<th>Country</th>
<th>Victims</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>United Kingdom</td>
<td>216,633</td>
</tr>
<tr>
<td>2</td>
<td>Canada</td>
<td>5,399</td>
</tr>
<tr>
<td>3</td>
<td>India</td>
<td>2,930</td>
</tr>
<tr>
<td>4</td>
<td>Greece</td>
<td>2,314</td>
</tr>
<tr>
<td>5</td>
<td>Australia</td>
<td>1,807</td>
</tr>
<tr>
<td>6</td>
<td>South Africa</td>
<td>1,754</td>
</tr>
<tr>
<td>7</td>
<td>France</td>
<td>1,640</td>
</tr>
<tr>
<td>8</td>
<td>Germany</td>
<td>1,578</td>
</tr>
<tr>
<td>9</td>
<td>Mexico</td>
<td>1,164</td>
</tr>
<tr>
<td>10</td>
<td>Belgium</td>
<td>1,023</td>
</tr>
<tr>
<td>11</td>
<td>Brazil</td>
<td>951</td>
</tr>
<tr>
<td>12</td>
<td>Philippines</td>
<td>898</td>
</tr>
<tr>
<td>13</td>
<td>Italy</td>
<td>728</td>
</tr>
<tr>
<td>14</td>
<td>Spain</td>
<td>618</td>
</tr>
<tr>
<td>15</td>
<td>Netherlands</td>
<td>450</td>
</tr>
<tr>
<td>16</td>
<td>Nigeria</td>
<td>443</td>
</tr>
<tr>
<td>17</td>
<td>Pakistan</td>
<td>443</td>
</tr>
<tr>
<td>18</td>
<td>China</td>
<td>442</td>
</tr>
<tr>
<td>19</td>
<td>Colombia</td>
<td>418</td>
</tr>
<tr>
<td>20</td>
<td>Hong Kong</td>
<td>407</td>
</tr>
</tbody>
</table>

Accessibility description: Image includes a world map with labels indicating the top 20 countries by number of total victims. The specific number of victims for each country are listed in descending order in the text table immediately below the image. Please see Appendix B for more information regarding IC3 data.
2020 - TOP 10 STATES BY NUMBER OF VICTIMS

Accessibility description: Image depicts a map of the United States. The top 10 states based on number of reporting victims are labeled. These include California, Florida, Texas, New York, Illinois, Pennsylvania, Washington, Nevada, New Jersey, and Maryland. Please see Appendix B for more information regarding IC3 data.

2020 - TOP 10 STATES BY VICTIM LOSS

Accessibility description: Image depicts a map of the United States. The top 10 states based on reported victim loss are labeled. These include California, New York, Texas, Florida, Ohio, Illinois, Missouri, Pennsylvania, Virginia, and Colorado. Please see Appendix B for more information regarding IC3 data.
## 2020 CRIME TYPES

### By Victim Count

<table>
<thead>
<tr>
<th>Crime Type</th>
<th>Victims</th>
<th>Crime Type</th>
<th>Victims</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phishing/Vishing/Smishing/Pharming</td>
<td>241,342</td>
<td>Other</td>
<td>10,372</td>
</tr>
<tr>
<td>Non-Payment/Non-Delivery</td>
<td>108,869</td>
<td>Investment</td>
<td>8,788</td>
</tr>
<tr>
<td>Extortion</td>
<td>76,741</td>
<td>Lottery/Sweepstakes/Inheritance</td>
<td>8,501</td>
</tr>
<tr>
<td>Personal Data Breach</td>
<td>45,330</td>
<td>IPR/Copyright and Counterfeit</td>
<td>4,213</td>
</tr>
<tr>
<td>Identity Theft</td>
<td>43,330</td>
<td>Crimes Against Children</td>
<td>3,202</td>
</tr>
<tr>
<td>Spoofing</td>
<td>28,218</td>
<td>Corporate Data Breach</td>
<td>2,794</td>
</tr>
<tr>
<td>Misrepresentation</td>
<td>24,276</td>
<td>Ransomware</td>
<td>2,474</td>
</tr>
<tr>
<td>Confidence Fraud/Romance</td>
<td>23,751</td>
<td>Denial of Service/TDoS</td>
<td>2,018</td>
</tr>
<tr>
<td>Harassment/Threats of Violence</td>
<td>20,604</td>
<td>Malware/Scareware/Virus</td>
<td>1,423</td>
</tr>
<tr>
<td>BEC/EAC</td>
<td>19,369</td>
<td>Health Care Related</td>
<td>1,383</td>
</tr>
<tr>
<td>Credit Card Fraud</td>
<td>17,614</td>
<td>Civil Matter</td>
<td>968</td>
</tr>
<tr>
<td>Employment</td>
<td>16,879</td>
<td>Re-shipping</td>
<td>883</td>
</tr>
<tr>
<td>Tech Support</td>
<td>15,421</td>
<td>Charity</td>
<td>659</td>
</tr>
<tr>
<td>Real Estate/Rental</td>
<td>13,638</td>
<td>Gambling</td>
<td>391</td>
</tr>
<tr>
<td>Advanced Fee</td>
<td>13,020</td>
<td>Terrorism</td>
<td>65</td>
</tr>
<tr>
<td>Government Impersonation</td>
<td>12,827</td>
<td>Hacktivist</td>
<td>52</td>
</tr>
<tr>
<td>Overpayment</td>
<td>10,988</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Descriptors*

<table>
<thead>
<tr>
<th>Descriptors*</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Social Media</td>
<td>35,439</td>
</tr>
<tr>
<td>Virtual Currency</td>
<td>35,229</td>
</tr>
</tbody>
</table>

*These descriptors relate to the medium or tool used to facilitate the crime and are used by the IC3 for tracking purposes only. They are available as descriptors only after another crime type has been selected. Please see Appendix B for more information regarding IC3 data.
## 2020 Crime Types Continued

### By Victim Loss

<table>
<thead>
<tr>
<th>Crime Type</th>
<th>Loss</th>
<th>Crime Type</th>
<th>Loss</th>
</tr>
</thead>
<tbody>
<tr>
<td>BEC/EAC</td>
<td>$1,866,642,107</td>
<td>Overpayment</td>
<td>$51,039,922</td>
</tr>
<tr>
<td>Confidence Fraud/Romance</td>
<td>$600,249,821</td>
<td>Ransomware</td>
<td><strong>$29,157,405</strong></td>
</tr>
<tr>
<td>Investment</td>
<td>$336,469,000</td>
<td>Health Care Related</td>
<td>$29,042,515</td>
</tr>
<tr>
<td>Non-Payment/Non-Delivery</td>
<td>$265,011,249</td>
<td>Civil Matter</td>
<td>$24,915,958</td>
</tr>
<tr>
<td>Identity Theft</td>
<td>$219,484,699</td>
<td>Misrepresentation</td>
<td>$19,707,242</td>
</tr>
<tr>
<td>Spoofing</td>
<td>$216,513,728</td>
<td>Malware/Scareware/Virus</td>
<td>$6,904,054</td>
</tr>
<tr>
<td>Real Estate/Rental</td>
<td>$213,196,082</td>
<td>Harassment/Threats Violence</td>
<td>$6,547,449</td>
</tr>
<tr>
<td>Personal Data Breach</td>
<td>$194,473,055</td>
<td>IPR/Copyright/Counterfeit</td>
<td>$5,910,617</td>
</tr>
<tr>
<td>Tech Support</td>
<td>$146,477,709</td>
<td>Charity</td>
<td>$4,428,766</td>
</tr>
<tr>
<td>Credit Card Fraud</td>
<td>$129,820,792</td>
<td>Gambling</td>
<td>$3,961,508</td>
</tr>
<tr>
<td>Corporate Data Breach</td>
<td>$128,916,648</td>
<td>Re-shipping</td>
<td>$3,095,265</td>
</tr>
<tr>
<td>Government Impersonation</td>
<td>$109,938,030</td>
<td>Crimes Against Children</td>
<td>$660,044</td>
</tr>
<tr>
<td>Other</td>
<td>$101,523,082</td>
<td>Denial of Service/TDos</td>
<td>$512,127</td>
</tr>
<tr>
<td>Advanced Fee</td>
<td>$83,215,405</td>
<td>Hacktivist</td>
<td>$50</td>
</tr>
<tr>
<td>Extortion</td>
<td>$70,935,939</td>
<td>Terrorism</td>
<td>$0</td>
</tr>
<tr>
<td>Employment</td>
<td>$62,314,015</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lottery/Sweepstakes/Inheritance</td>
<td>$61,111,319</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Phishing/Vishing/Smishing/Pharming</td>
<td>$54,241,075</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Descriptors*

<table>
<thead>
<tr>
<th>Descriptors*</th>
<th>Loss</th>
</tr>
</thead>
<tbody>
<tr>
<td>Social Media</td>
<td>$155,323,073</td>
</tr>
<tr>
<td>Virtual Currency</td>
<td>$246,212,432</td>
</tr>
</tbody>
</table>

*These descriptors relate to the medium or tool used to facilitate the crime and are used by the IC3 for tracking purposes only. They are available only after another crime type has been selected. Please see Appendix B for more information regarding IC3 data.

---

** Regarding ransomware adjusted losses, this number does not include estimates of lost business, time, wages, files, or equipment, or any third-party remediation services acquired by a victim. In some cases, victims do not report any loss amount to the FBI, thereby creating an artificially low overall ransomware loss rate. Lastly, the number only represents what victims report to the FBI via the IC3 and does not account for victim direct reporting to FBI field offices/agents.
## Last 3 Year Complaint Count Comparison

### By Victim Count

<table>
<thead>
<tr>
<th>Crime Type</th>
<th>2020</th>
<th>2019</th>
<th>2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced Fee</td>
<td>13,020</td>
<td>14,607</td>
<td>16,362</td>
</tr>
<tr>
<td>BEC/EAC</td>
<td>19,369</td>
<td>23,775</td>
<td>20,373</td>
</tr>
<tr>
<td>Charity</td>
<td>659</td>
<td>407</td>
<td>493</td>
</tr>
<tr>
<td>Civil Matter</td>
<td>968</td>
<td>908</td>
<td>768</td>
</tr>
<tr>
<td>Confidence Fraud/Romance</td>
<td>23,751</td>
<td>19,473</td>
<td>18,493</td>
</tr>
<tr>
<td>Corporate Data Breach</td>
<td>2,794</td>
<td>1,795</td>
<td>2,480</td>
</tr>
<tr>
<td>Credit Card Fraud</td>
<td>17,614</td>
<td>14,378</td>
<td>15,210</td>
</tr>
<tr>
<td>Crimes Against Children</td>
<td>3,202</td>
<td>1,312</td>
<td>1,394</td>
</tr>
<tr>
<td>Denial of Service/TDoS</td>
<td>2,018</td>
<td>1,353</td>
<td>1,799</td>
</tr>
<tr>
<td>Employment</td>
<td>16,879</td>
<td>14,493</td>
<td>14,979</td>
</tr>
<tr>
<td>Extortion</td>
<td>76,741</td>
<td>43,101</td>
<td>51,146</td>
</tr>
<tr>
<td>Gambling</td>
<td>391</td>
<td>262</td>
<td>181</td>
</tr>
<tr>
<td>Government Impersonation</td>
<td>12,827</td>
<td>13,873</td>
<td>10,978</td>
</tr>
<tr>
<td>Hacktivist</td>
<td>52</td>
<td>39</td>
<td>77</td>
</tr>
<tr>
<td>Harassment/Threats of Violence</td>
<td>20,604</td>
<td>15,502</td>
<td>18,415</td>
</tr>
<tr>
<td>Health Care Related</td>
<td>1,383</td>
<td>657</td>
<td>337</td>
</tr>
<tr>
<td>Identity Theft</td>
<td>43,330</td>
<td>16,053</td>
<td>16,128</td>
</tr>
<tr>
<td>Investment</td>
<td>8,788</td>
<td>3,999</td>
<td>3,693</td>
</tr>
<tr>
<td>IPR/Copyright and Counterfeit</td>
<td>4,213</td>
<td>3,892</td>
<td>2,249</td>
</tr>
<tr>
<td>Lottery/Sweepstakes/Inheritance</td>
<td>8,501</td>
<td>7,767</td>
<td>7,146</td>
</tr>
<tr>
<td>Malware/Scareware/Virus</td>
<td>1,423</td>
<td>2,373</td>
<td>2,811</td>
</tr>
<tr>
<td>Misrepresentation</td>
<td>24,276</td>
<td>5,975</td>
<td>5,959</td>
</tr>
<tr>
<td>Non-Payment/Non-Delivery</td>
<td>108,869</td>
<td>61,832</td>
<td>65,116</td>
</tr>
<tr>
<td>Other</td>
<td>10,372</td>
<td>10,842</td>
<td>10,826</td>
</tr>
<tr>
<td>Overpayment</td>
<td>10,988</td>
<td>15,395</td>
<td>15,512</td>
</tr>
<tr>
<td>Personal Data Breach</td>
<td>45,330</td>
<td>38,218</td>
<td>50,642</td>
</tr>
<tr>
<td>Phishing/Vishing/Smishing/Pharming</td>
<td>241,342</td>
<td>114,702</td>
<td>26,379</td>
</tr>
<tr>
<td>Ransomware</td>
<td>2,474</td>
<td>2,047</td>
<td>1,493</td>
</tr>
<tr>
<td>Real Estate/Rental</td>
<td>13,638</td>
<td>11,677</td>
<td>11,300</td>
</tr>
<tr>
<td>Re-Shipping</td>
<td>883</td>
<td>929</td>
<td>907</td>
</tr>
<tr>
<td>Spoofing</td>
<td>28,218</td>
<td>25,789</td>
<td>15,569</td>
</tr>
<tr>
<td>Tech Support</td>
<td>15,421</td>
<td>13,633</td>
<td>14,408</td>
</tr>
<tr>
<td>Terrorism</td>
<td>65</td>
<td>61</td>
<td>120</td>
</tr>
</tbody>
</table>
## Last 3 Year Complaint Loss Comparison Continued

### By Victim Loss

<table>
<thead>
<tr>
<th>Crime Type</th>
<th>2020</th>
<th>2019</th>
<th>2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced Fee</td>
<td>$83,215,405</td>
<td>$100,602,297</td>
<td>$92,271,682</td>
</tr>
<tr>
<td>BEC/EAC</td>
<td>$1,866,642,107</td>
<td>$1,776,549,688</td>
<td>$1,297,803,489</td>
</tr>
<tr>
<td>Charity</td>
<td>$4,428,766</td>
<td>$2,214,383</td>
<td>$1,006,379</td>
</tr>
<tr>
<td>Civil Matter</td>
<td>$24,915,958</td>
<td>$20,242,867</td>
<td>$15,172,692</td>
</tr>
<tr>
<td>Confidence Fraud/Romance</td>
<td>$600,249,821</td>
<td>$475,014,032</td>
<td>$362,500,761</td>
</tr>
<tr>
<td>Corporate Data Breach</td>
<td>$128,916,648</td>
<td>$53,398,278</td>
<td>$117,711,989</td>
</tr>
<tr>
<td>Credit Card Fraud</td>
<td>$129,820,792</td>
<td>$111,491,163</td>
<td>$88,991,436</td>
</tr>
<tr>
<td>Crimes Against Children</td>
<td>$660,044</td>
<td>$975,311</td>
<td>$265,996</td>
</tr>
<tr>
<td>Denial of Service/TDoS</td>
<td>$512,127</td>
<td>$7,598,198</td>
<td>$2,052,340</td>
</tr>
<tr>
<td>Employment</td>
<td>$62,314,015</td>
<td>$42,618,705</td>
<td>$45,487,120</td>
</tr>
<tr>
<td>Extortion</td>
<td>$70,935,939</td>
<td>$107,498,956</td>
<td>$83,357,901</td>
</tr>
<tr>
<td>Gambling</td>
<td>$3,961,508</td>
<td>$1,458,118</td>
<td>$926,953</td>
</tr>
<tr>
<td>Government Impersonation</td>
<td>$109,938,030</td>
<td>$124,292,606</td>
<td>$64,211,765</td>
</tr>
<tr>
<td>Hacktivist</td>
<td>$50</td>
<td>$129,000</td>
<td>$77,612</td>
</tr>
<tr>
<td>Harassment/Threats of Violence</td>
<td>$6,547,449</td>
<td>$19,866,654</td>
<td>$21,903,829</td>
</tr>
<tr>
<td>Health Care Related</td>
<td>$29,042,515</td>
<td>$1,128,838</td>
<td>$4,474,792</td>
</tr>
<tr>
<td>Identity Theft</td>
<td>$219,484,699</td>
<td>$160,305,789</td>
<td>$100,429,691</td>
</tr>
<tr>
<td>Investment</td>
<td>$336,469,000</td>
<td>$222,186,195</td>
<td>$252,955,320</td>
</tr>
<tr>
<td>IPR/Copyright and Counterfeit</td>
<td>$5,910,617</td>
<td>$10,293,307</td>
<td>$15,802,011</td>
</tr>
<tr>
<td>Lottery/Sweepstakes/Inheritance</td>
<td>$61,111,319</td>
<td>$48,642,332</td>
<td>$60,214,814</td>
</tr>
<tr>
<td>Malware/Scareware/Virus</td>
<td>$6,904,054</td>
<td>$2,009,119</td>
<td>$7,411,651</td>
</tr>
<tr>
<td>Misrepresentation</td>
<td>$19,707,242</td>
<td>$12,371,573</td>
<td>$20,000,713</td>
</tr>
<tr>
<td>Non-Payment/Non-Delivery</td>
<td>$265,011,249</td>
<td>$196,563,497</td>
<td>$183,826,809</td>
</tr>
<tr>
<td>Other</td>
<td>$101,523,082</td>
<td>$66,223,160</td>
<td>$63,126,929</td>
</tr>
<tr>
<td>Overpayment</td>
<td>$51,039,922</td>
<td>$55,820,212</td>
<td>$53,225,507</td>
</tr>
<tr>
<td>Personal Data Breach</td>
<td>$194,473,055</td>
<td>$120,102,501</td>
<td>$148,892,403</td>
</tr>
<tr>
<td>Phishing/Vishing/Smishing/Pharming</td>
<td>$54,241,075</td>
<td>$57,836,379</td>
<td>$48,241,748</td>
</tr>
<tr>
<td>Ransomware</td>
<td>$29,157,405</td>
<td>$8,965,847</td>
<td>$3,621,857</td>
</tr>
<tr>
<td>Real Estate/Rental</td>
<td>$213,196,082</td>
<td>$221,365,911</td>
<td>$149,458,114</td>
</tr>
<tr>
<td>Re-Shipping</td>
<td>$3,095,265</td>
<td>$1,772,692</td>
<td>$1,684,179</td>
</tr>
<tr>
<td>Spoofing</td>
<td>$216,513,728</td>
<td>$300,478,433</td>
<td>$70,000,248</td>
</tr>
<tr>
<td>Tech Support</td>
<td>$146,477,709</td>
<td>$54,041,053</td>
<td>$38,697,026</td>
</tr>
<tr>
<td>Terrorism</td>
<td>$0</td>
<td>$49,589</td>
<td>$10,193</td>
</tr>
</tbody>
</table>
# 2020 Overall State Statistics

## Victim per State*

<table>
<thead>
<tr>
<th>Rank</th>
<th>State</th>
<th>Victims</th>
<th>Rank</th>
<th>State</th>
<th>Victims</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>California</td>
<td>69,541</td>
<td>30</td>
<td>Louisiana</td>
<td>5,077</td>
</tr>
<tr>
<td>2</td>
<td>Florida</td>
<td>53,793</td>
<td>31</td>
<td>Utah</td>
<td>4,926</td>
</tr>
<tr>
<td>3</td>
<td>Texas</td>
<td>38,640</td>
<td>32</td>
<td>Oklahoma</td>
<td>4,785</td>
</tr>
<tr>
<td>4</td>
<td>New York</td>
<td>34,505</td>
<td>33</td>
<td>Arkansas</td>
<td>4,237</td>
</tr>
<tr>
<td>5</td>
<td>Illinois</td>
<td>20,185</td>
<td>34</td>
<td>Kansas</td>
<td>3,457</td>
</tr>
<tr>
<td>6</td>
<td>Pennsylvania</td>
<td>18,636</td>
<td>35</td>
<td>New Mexico</td>
<td>3,427</td>
</tr>
<tr>
<td>7</td>
<td>Washington</td>
<td>17,229</td>
<td>36</td>
<td>Mississippi</td>
<td>2,478</td>
</tr>
<tr>
<td>8</td>
<td>Nevada</td>
<td>16,110</td>
<td>37</td>
<td>Delaware</td>
<td>2,230</td>
</tr>
<tr>
<td>9</td>
<td>New Jersey</td>
<td>14,829</td>
<td>38</td>
<td>Idaho</td>
<td>2,209</td>
</tr>
<tr>
<td>10</td>
<td>Maryland</td>
<td>14,804</td>
<td>39</td>
<td>Nebraska</td>
<td>2,166</td>
</tr>
<tr>
<td>11</td>
<td>Virginia</td>
<td>13,770</td>
<td>40</td>
<td>District of Columbia</td>
<td>2,132</td>
</tr>
<tr>
<td>12</td>
<td>Ohio</td>
<td>13,421</td>
<td>41</td>
<td>Alaska</td>
<td>2,073</td>
</tr>
<tr>
<td>13</td>
<td>Georgia</td>
<td>13,402</td>
<td>42</td>
<td>New Hampshire</td>
<td>2,015</td>
</tr>
<tr>
<td>14</td>
<td>Arizona</td>
<td>13,009</td>
<td>43</td>
<td>Hawaii</td>
<td>1,978</td>
</tr>
<tr>
<td>15</td>
<td>Indiana</td>
<td>12,786</td>
<td>44</td>
<td>West Virginia</td>
<td>1,902</td>
</tr>
<tr>
<td>16</td>
<td>Michigan</td>
<td>12,521</td>
<td>45</td>
<td>Puerto Rico</td>
<td>1,886</td>
</tr>
<tr>
<td>17</td>
<td>Colorado</td>
<td>12,325</td>
<td>46</td>
<td>Rhode Island</td>
<td>1,677</td>
</tr>
<tr>
<td>18</td>
<td>North Carolina</td>
<td>12,223</td>
<td>47</td>
<td>Maine</td>
<td>1,672</td>
</tr>
<tr>
<td>19</td>
<td>Massachusetts</td>
<td>11,468</td>
<td>48</td>
<td>Montana</td>
<td>1,365</td>
</tr>
<tr>
<td>20</td>
<td>Iowa</td>
<td>9,367</td>
<td>49</td>
<td>Wyoming</td>
<td>913</td>
</tr>
<tr>
<td>21</td>
<td>Tennessee</td>
<td>8,527</td>
<td>50</td>
<td>Vermont</td>
<td>856</td>
</tr>
<tr>
<td>22</td>
<td>Wisconsin</td>
<td>8,308</td>
<td>51</td>
<td>South Dakota</td>
<td>777</td>
</tr>
<tr>
<td>23</td>
<td>Missouri</td>
<td>8,160</td>
<td>52</td>
<td>North Dakota</td>
<td>760</td>
</tr>
<tr>
<td>24</td>
<td>Minnesota</td>
<td>6,847</td>
<td>53</td>
<td>U.S. Minor Outlying Islands</td>
<td>116</td>
</tr>
<tr>
<td>25</td>
<td>Oregon</td>
<td>6,817</td>
<td>54</td>
<td>Guam</td>
<td>112</td>
</tr>
<tr>
<td>26</td>
<td>Kentucky</td>
<td>6,815</td>
<td>55</td>
<td>Virgin Islands, U.S.</td>
<td>92</td>
</tr>
<tr>
<td>27</td>
<td>South Carolina</td>
<td>5,853</td>
<td>56</td>
<td>American Samoa</td>
<td>42</td>
</tr>
<tr>
<td>28</td>
<td>Alabama</td>
<td>5,803</td>
<td>57</td>
<td>Northern Mariana Islands</td>
<td>20</td>
</tr>
<tr>
<td>29</td>
<td>Connecticut</td>
<td>5,636</td>
<td>77</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Note: This information is based on the total number of complaints from each state, American Territory, and the District of Columbia when the complainant provided state information. Please see Appendix B for more information regarding IC3 data.
## 2020 Overall State Statistics Continued

### Total Victim Losses by State*

<table>
<thead>
<tr>
<th>Rank</th>
<th>State</th>
<th>Loss</th>
<th>Rank</th>
<th>State</th>
<th>Loss</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>California</td>
<td>$621,452,320</td>
<td>30</td>
<td>South Carolina</td>
<td>$25,244,978</td>
</tr>
<tr>
<td>2</td>
<td>New York</td>
<td>$415,812,917</td>
<td>31</td>
<td>New Mexico</td>
<td>$23,903,594</td>
</tr>
<tr>
<td>3</td>
<td>Texas</td>
<td>$313,565,225</td>
<td>32</td>
<td>Iowa</td>
<td>$21,396,701</td>
</tr>
<tr>
<td>4</td>
<td>Florida</td>
<td>$295,032,829</td>
<td>33</td>
<td>Oklahoma</td>
<td>$20,748,692</td>
</tr>
<tr>
<td>5</td>
<td>Ohio</td>
<td>$170,171,951</td>
<td>34</td>
<td>Kansas</td>
<td>$19,157,289</td>
</tr>
<tr>
<td>6</td>
<td>Illinois</td>
<td>$150,496,678</td>
<td>35</td>
<td>District of Columbia</td>
<td>$18,942,722</td>
</tr>
<tr>
<td>7</td>
<td>Missouri</td>
<td>$115,913,584</td>
<td>36</td>
<td>Mississippi</td>
<td>$18,111,738</td>
</tr>
<tr>
<td>8</td>
<td>Pennsylvania</td>
<td>$108,506,204</td>
<td>37</td>
<td>Iowa</td>
<td>$17,371,515</td>
</tr>
<tr>
<td>9</td>
<td>Alabama</td>
<td>$98,762,523</td>
<td>38</td>
<td>North Carolina</td>
<td>$16,671,531</td>
</tr>
<tr>
<td>10</td>
<td>Virginia</td>
<td>$98,727,053</td>
<td>39</td>
<td>Puerto Rico</td>
<td>$15,275,104</td>
</tr>
<tr>
<td>11</td>
<td>Georgia</td>
<td>$98,727,053</td>
<td>40</td>
<td>Idaho</td>
<td>$14,670,650</td>
</tr>
<tr>
<td>12</td>
<td>New Jersey</td>
<td>$98,727,053</td>
<td>41</td>
<td>Nebraska</td>
<td>$13,799,640</td>
</tr>
<tr>
<td>13</td>
<td>Massachusetts</td>
<td>$97,583,753</td>
<td>42</td>
<td>Rhode Island</td>
<td>$12,590,784</td>
</tr>
<tr>
<td>14</td>
<td>Washington</td>
<td>$88,020,254</td>
<td>43</td>
<td>American Samoa</td>
<td>$7,806,373</td>
</tr>
<tr>
<td>15</td>
<td>Michigan</td>
<td>$83,999,442</td>
<td>44</td>
<td>Iowa</td>
<td>$7,669,670</td>
</tr>
<tr>
<td>16</td>
<td>Arizona</td>
<td>$72,128,637</td>
<td>45</td>
<td>Alaska</td>
<td>$7,342,743</td>
</tr>
<tr>
<td>17</td>
<td>North Carolina</td>
<td>$69,409,152</td>
<td>46</td>
<td>Maine</td>
<td>$7,073,260</td>
</tr>
<tr>
<td>18</td>
<td>Maryland</td>
<td>$62,473,193</td>
<td>47</td>
<td>Delaware</td>
<td>$6,486,617</td>
</tr>
<tr>
<td>19</td>
<td>Minnesota</td>
<td>$58,341,798</td>
<td>48</td>
<td>Montana</td>
<td>$5,669,293</td>
</tr>
<tr>
<td>20</td>
<td>Utah</td>
<td>$47,113,946</td>
<td>49</td>
<td>Wyoming</td>
<td>$5,096,704</td>
</tr>
<tr>
<td>21</td>
<td>Nevada</td>
<td>$44,383,452</td>
<td>50</td>
<td>New Hampshire</td>
<td>$4,949,296</td>
</tr>
<tr>
<td>22</td>
<td>Connecticut</td>
<td>$41,311,798</td>
<td>51</td>
<td>West Virginia</td>
<td>$4,823,786</td>
</tr>
<tr>
<td>23</td>
<td>Tennessee</td>
<td>$40,191,616</td>
<td>52</td>
<td>Vermont</td>
<td>$4,175,799</td>
</tr>
<tr>
<td>24</td>
<td>Oregon</td>
<td>$38,389,702</td>
<td>53</td>
<td>South Dakota</td>
<td>$3,208,241</td>
</tr>
<tr>
<td>25</td>
<td>Wisconsin</td>
<td>$36,081,681</td>
<td>54</td>
<td>Virgin Islands, U.S.</td>
<td>$620,962</td>
</tr>
<tr>
<td>26</td>
<td>Indiana</td>
<td>$35,180,105</td>
<td>55</td>
<td>Guam</td>
<td>$259,338</td>
</tr>
<tr>
<td>27</td>
<td>Alabama</td>
<td>$27,549,157</td>
<td>56</td>
<td>U.S. Minor Outlying Islands</td>
<td>$201,022</td>
</tr>
<tr>
<td>28</td>
<td>Louisiana</td>
<td>$26,717,928</td>
<td>57</td>
<td>Northern Mariana Islands</td>
<td>$67,403</td>
</tr>
<tr>
<td>29</td>
<td>North Dakota</td>
<td>$25,804,940</td>
<td>58</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Note: This information is based on the total number of complaints from each state, American Territory, and the District of Columbia when the complainant provided state information. Please see Appendix B for more information regarding IC3 data.
## Count by Subject per State*

<table>
<thead>
<tr>
<th>Rank</th>
<th>State</th>
<th>Subjects</th>
<th>Rank</th>
<th>State</th>
<th>Subjects</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>California</td>
<td>26,379</td>
<td>30</td>
<td>Utah</td>
<td>1,251</td>
</tr>
<tr>
<td>2</td>
<td>Florida</td>
<td>19,364</td>
<td>31</td>
<td>Louisiana</td>
<td>1,246</td>
</tr>
<tr>
<td>3</td>
<td>Texas</td>
<td>12,914</td>
<td>32</td>
<td>District of Columbia</td>
<td>1,174</td>
</tr>
<tr>
<td>4</td>
<td>New Jersey</td>
<td>10,616</td>
<td>33</td>
<td>Kentucky</td>
<td>1,146</td>
</tr>
<tr>
<td>5</td>
<td>New York</td>
<td>10,052</td>
<td>34</td>
<td>Delaware</td>
<td>1,096</td>
</tr>
<tr>
<td>6</td>
<td>Maryland</td>
<td>7,279</td>
<td>35</td>
<td>Kansas</td>
<td>1,090</td>
</tr>
<tr>
<td>7</td>
<td>Illinois</td>
<td>4,780</td>
<td>36</td>
<td>Connecticut</td>
<td>969</td>
</tr>
<tr>
<td>8</td>
<td>Georgia</td>
<td>4,321</td>
<td>37</td>
<td>New Mexico</td>
<td>890</td>
</tr>
<tr>
<td>9</td>
<td>Pennsylvania</td>
<td>4,066</td>
<td>38</td>
<td>Mississippi</td>
<td>824</td>
</tr>
<tr>
<td>10</td>
<td>Virginia</td>
<td>3,929</td>
<td>39</td>
<td>Arkansas</td>
<td>784</td>
</tr>
<tr>
<td>11</td>
<td>Washington</td>
<td>3,807</td>
<td>40</td>
<td>Iowa</td>
<td>721</td>
</tr>
<tr>
<td>12</td>
<td>Ohio</td>
<td>3,708</td>
<td>41</td>
<td>Maine</td>
<td>691</td>
</tr>
<tr>
<td>13</td>
<td>Nevada</td>
<td>3,707</td>
<td>42</td>
<td>Hawaii</td>
<td>490</td>
</tr>
<tr>
<td>14</td>
<td>Arizona</td>
<td>3,005</td>
<td>43</td>
<td>West Virginia</td>
<td>449</td>
</tr>
<tr>
<td>15</td>
<td>North Carolina</td>
<td>2,940</td>
<td>44</td>
<td>Idaho</td>
<td>448</td>
</tr>
<tr>
<td>16</td>
<td>Michigan</td>
<td>2,793</td>
<td>45</td>
<td>North Dakota</td>
<td>425</td>
</tr>
<tr>
<td>17</td>
<td>Colorado</td>
<td>2,502</td>
<td>46</td>
<td>New Hampshire</td>
<td>360</td>
</tr>
<tr>
<td>18</td>
<td>Tennessee</td>
<td>2,480</td>
<td>47</td>
<td>Puerto Rico</td>
<td>330</td>
</tr>
<tr>
<td>19</td>
<td>Indiana</td>
<td>2,211</td>
<td>48</td>
<td>Rhode Island</td>
<td>330</td>
</tr>
<tr>
<td>20</td>
<td>Massachusetts</td>
<td>2,192</td>
<td>49</td>
<td>Alaska</td>
<td>292</td>
</tr>
<tr>
<td>21</td>
<td>Missouri</td>
<td>1,824</td>
<td>50</td>
<td>Wyoming</td>
<td>277</td>
</tr>
<tr>
<td>22</td>
<td>Nebraska</td>
<td>1,734</td>
<td>51</td>
<td>South Dakota</td>
<td>213</td>
</tr>
<tr>
<td>23</td>
<td>Oklahoma</td>
<td>1,721</td>
<td>52</td>
<td>Vermont</td>
<td>172</td>
</tr>
<tr>
<td>24</td>
<td>Minnesota</td>
<td>1,699</td>
<td>53</td>
<td>U.S. Minor Outlying Islands</td>
<td>32</td>
</tr>
<tr>
<td>25</td>
<td>Alabama</td>
<td>1,574</td>
<td>54</td>
<td>Guam</td>
<td>22</td>
</tr>
<tr>
<td>26</td>
<td>Oregon</td>
<td>1,543</td>
<td>55</td>
<td>Virgin Islands, U.S.</td>
<td>18</td>
</tr>
<tr>
<td>27</td>
<td>Montana</td>
<td>1,507</td>
<td>56</td>
<td>American Samoa</td>
<td>6</td>
</tr>
<tr>
<td>28</td>
<td>Wisconsin</td>
<td>1,342</td>
<td>57</td>
<td>Northern Mariana Islands</td>
<td>2</td>
</tr>
<tr>
<td>29</td>
<td>South Carolina</td>
<td>1,341</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Note: This information is based on the total number of complaints from each state, American Territory, and the District of Columbia when the complainant provided state information. Please see Appendix B for more information regarding IC3 data.
### 2020 Overall State Statistics Continued

#### Subject Earnings per Destination State*

<table>
<thead>
<tr>
<th>Rank</th>
<th>State</th>
<th>Loss</th>
<th>Rank</th>
<th>State</th>
<th>Loss</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>California</td>
<td>$233,907,224</td>
<td>30</td>
<td>Oregon</td>
<td>$9,473,549</td>
</tr>
<tr>
<td>2</td>
<td>New York</td>
<td>$142,689,230</td>
<td>31</td>
<td>Missouri</td>
<td>$9,322,612</td>
</tr>
<tr>
<td>3</td>
<td>Texas</td>
<td>$135,573,752</td>
<td>32</td>
<td>Utah</td>
<td>$9,225,351</td>
</tr>
<tr>
<td>4</td>
<td>Florida</td>
<td>$125,049,181</td>
<td>33</td>
<td>Kansas</td>
<td>$9,205,096</td>
</tr>
<tr>
<td>5</td>
<td>Ohio</td>
<td>$83,544,428</td>
<td>34</td>
<td>Wisconsin</td>
<td>$8,357,864</td>
</tr>
<tr>
<td>6</td>
<td>Georgia</td>
<td>$63,933,271</td>
<td>35</td>
<td>Kentucky</td>
<td>$6,623,738</td>
</tr>
<tr>
<td>7</td>
<td>Illinois</td>
<td>$52,691,430</td>
<td>36</td>
<td>Iowa</td>
<td>$6,253,965</td>
</tr>
<tr>
<td>8</td>
<td>Washington</td>
<td>$47,175,498</td>
<td>37</td>
<td>Maine</td>
<td>$6,138,289</td>
</tr>
<tr>
<td>9</td>
<td>Colorado</td>
<td>$42,901,870</td>
<td>38</td>
<td>Alaska</td>
<td>$5,785,807</td>
</tr>
<tr>
<td>10</td>
<td>New Jersey</td>
<td>$38,491,372</td>
<td>39</td>
<td>New Mexico</td>
<td>$5,711,844</td>
</tr>
<tr>
<td>11</td>
<td>Maryland</td>
<td>$29,971,760</td>
<td>40</td>
<td>Delaware</td>
<td>$5,673,719</td>
</tr>
<tr>
<td>12</td>
<td>Nevada</td>
<td>$29,127,283</td>
<td>41</td>
<td>Nebraska</td>
<td>$5,651,920</td>
</tr>
<tr>
<td>13</td>
<td>Arizona</td>
<td>$28,473,605</td>
<td>42</td>
<td>Mississippi</td>
<td>$3,978,526</td>
</tr>
<tr>
<td>14</td>
<td>Pennsylvania</td>
<td>$28,431,645</td>
<td>43</td>
<td>New Hampshire</td>
<td>$3,595,627</td>
</tr>
<tr>
<td>15</td>
<td>Virginia</td>
<td>$25,657,584</td>
<td>44</td>
<td>Idaho</td>
<td>$3,582,262</td>
</tr>
<tr>
<td>16</td>
<td>Michigan</td>
<td>$24,395,899</td>
<td>45</td>
<td>Hawaii</td>
<td>$3,168,489</td>
</tr>
<tr>
<td>17</td>
<td>North Dakota</td>
<td>$22,018,169</td>
<td>46</td>
<td>Arkansas</td>
<td>$2,546,501</td>
</tr>
<tr>
<td>18</td>
<td>North Carolina</td>
<td>$20,552,835</td>
<td>47</td>
<td>South Dakota</td>
<td>$2,486,492</td>
</tr>
<tr>
<td>19</td>
<td>District of Columbia</td>
<td>$14,479,130</td>
<td>48</td>
<td>Wyoming</td>
<td>$2,337,866</td>
</tr>
<tr>
<td>20</td>
<td>Massachusetts</td>
<td>$14,295,694</td>
<td>49</td>
<td>Rhode Island</td>
<td>$2,013,255</td>
</tr>
<tr>
<td>21</td>
<td>Oklahoma</td>
<td>$13,036,365</td>
<td>50</td>
<td>Vermont</td>
<td>$1,506,113</td>
</tr>
<tr>
<td>22</td>
<td>Indiana</td>
<td>$12,864,230</td>
<td>51</td>
<td>Puerto Rico</td>
<td>$1,422,863</td>
</tr>
<tr>
<td>23</td>
<td>Connecticut</td>
<td>$12,533,843</td>
<td>52</td>
<td>West Virginia</td>
<td>$1,352,504</td>
</tr>
<tr>
<td>24</td>
<td>Tennessee</td>
<td>$12,017,224</td>
<td>53</td>
<td>Virgin Islands, U.S.</td>
<td>$248,287</td>
</tr>
<tr>
<td>25</td>
<td>Louisiana</td>
<td>$11,932,340</td>
<td>54</td>
<td>U.S. Minor Outlying Islands</td>
<td>$225,488</td>
</tr>
<tr>
<td>26</td>
<td>Minnesota</td>
<td>$11,920,258</td>
<td>55</td>
<td>Guam</td>
<td>$12,520</td>
</tr>
<tr>
<td>27</td>
<td>Alabama</td>
<td>$10,739,652</td>
<td>56</td>
<td>American Samoa</td>
<td>$494</td>
</tr>
<tr>
<td>28</td>
<td>Montana</td>
<td>$10,262,099</td>
<td>57</td>
<td>Northern Mariana Islands</td>
<td>$315</td>
</tr>
<tr>
<td>29</td>
<td>South Carolina</td>
<td>$10,063,305</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Note: This information is based on the total number of complaints from each state, American Territory, and the District of Columbia when the complainant provided state information. Please see Appendix B for more information regarding IC3 data.*
APPENDIX A: DEFINITIONS

Overpayment: An individual is sent a payment/commission and is instructed to keep a portion of the payment and send the remainder to another individual or business.

Advanced Fee: An individual pays money to someone in anticipation of receiving something of greater value in return, but instead, receives significantly less than expected or nothing.

Business Email Compromise/Email Account Compromise: BEC is a scam targeting businesses (not individuals) working with foreign suppliers and/or businesses regularly performing wire transfer payments. EAC is a similar scam which targets individuals. These sophisticated scams are carried out by fraudsters compromising email accounts through social engineering or computer intrusion techniques to conduct unauthorized transfer of funds.

Charity: Perpetrators set up false charities, usually following natural disasters, and profit from individuals who believe they are making donations to legitimate charitable organizations.

Civil Matter: Civil litigation generally includes all disputes formally submitted to a court, about any subject in which one party is claimed to have committed a wrong but not a crime. In general, this is the legal process most people think of when the word “lawsuit” is used.

Confidence/Romance Fraud: An individual believes they are in a relationship (family, friendly, or romantic) and are tricked into sending money, personal and financial information, or items of value to the perpetrator or to launder money or items to assist the perpetrator. This includes the Grandparent’s Scheme and any scheme in which the perpetrator preys on the complainant’s “heartstrings”.

Corporate Data Breach: A leak or spill of business data that is released from a secure location to an untrusted environment. It may also refer to a data breach within a corporation or business where sensitive, protected, or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorized to do so.

Credit Card Fraud: Credit card fraud is a wide-ranging term for theft and fraud committed using a credit card or any similar payment mechanism (ACH, EFT, recurring charge, etc.) as a fraudulent source of funds in a transaction.

Crimes Against Children: Anything related to the exploitation of children, including child abuse.

Denial of Service/TDoS: A Denial of Service (DoS) attack floods a network/system or a Telephony Denial of Service (TDoS) floods a voice service with multiple requests, slowing down or interrupting service.

Employment: An individual believes they are legitimately employed and loses money, or launders money/items during the course of their employment.

Extortion: Unlawful extraction of money or property through intimidation or undue exercise of authority. It may include threats of physical harm, criminal prosecution, or public exposure.

Gambling: Online gambling, also known as Internet gambling and iGambling, is a general term for gambling using the Internet.

Government Impersonation: A government official is impersonated in an attempt to collect money.
**Hacktivist:** A computer hacker whose activity is aimed at promoting a social or political cause.

**Harassment/Threats of Violence:** Harassment occurs when a perpetrator uses false accusations or statements of fact to intimidate a victim. Threats of Violence refers to an expression of an intention to inflict pain, injury, or punishment, which does not refer to the requirement of payment.

**Health Care Related:** A scheme attempting to defraud private or government health care programs which usually involving health care providers, companies, or individuals. Schemes may include offers for fake insurance cards, health insurance marketplace assistance, stolen health information, or various other scams and/or any scheme involving medications, supplements, weight loss products, or diversion/pill mill practices. These scams are often initiated through spam email, Internet advertisements, links in forums/social media, and fraudulent websites.

**IPR/Copyright and Counterfeit:** The illegal theft and use of others’ ideas, inventions, and creative expressions – what’s called intellectual property – everything from trade secrets and proprietary products and parts to movies, music, and software.

**Identity Theft:** Someone steals and uses personal identifying information, like a name or Social Security number, without permission to commit fraud or other crimes and/or (Account Takeover) a fraudster obtains account information to perpetrate fraud on existing accounts.

**Investment:** Deceptive practice that induces investors to make purchases on the basis of false information. These scams usually offer the victims large returns with minimal risk. (Retirement, 401K, Ponzi, Pyramid, etc.).

**Lottery/Sweepstakes/Inheritance:** An Individual is contacted about winning a lottery or sweepstakes they never entered, or to collect on an inheritance from an unknown relative.

**Malware/Scareware/Virus:** Software or code intended to damage, disable, or capable of copying itself onto a computer and/or computer systems to have a detrimental effect or destroy data.

**Misrepresentation:** Merchandise or services were purchased or contracted by individuals online for which the purchasers provided payment. The goods or services received were of a measurably lesser quality or quantity than was described by the seller.

**Non-Payment/Non-Delivery:** In non-payment situations, goods and services are shipped, but payment is never rendered. In non-delivery situations, payment is sent, but goods and services are never received.

**Personal Data Breach:** A leak/spill of personal data which is released from a secure location to an untrusted environment. Also, a security incident in which an individual’s sensitive, protected, or confidential data is copied, transmitted, viewed, stolen or used by an unauthorized individual.

**Phishing/Vishing/Smishing/Pharming:** The use of unsolicited email, text messages, and telephone calls purportedly from a legitimate company requesting personal, financial, and/or login credentials.

**Ransomware:** A type of malicious software designed to block access to a computer system until money is paid.

**Re-shipping:** Individuals receive packages at their residence and subsequently repackage the merchandise for shipment, usually abroad.
**Real Estate/Rental**: Loss of funds from a real estate investment or fraud involving rental or timeshare property.

**Spoofing**: Contact information (phone number, email, and website) is deliberately falsified to mislead and appear to be from a legitimate source. For example, spoofed phone numbers making mass robocalls; spoofed emails sending mass spam; forged websites used to mislead and gather personal information. Often used in connection with other crime types.

**Social Media**: A complaint alleging the use of social networking or social media (Facebook, Twitter, Instagram, chat rooms, etc.) as a vector for fraud. Social Media does not include dating sites.

**Tech Support**: Subject posing as technical or customer support/service.

**Terrorism**: Violent acts intended to create fear that are perpetrated for a religious, political, or ideological goal and deliberately target or disregard the safety of non-combatants.

**Virtual Currency**: A complaint mentioning a form of virtual cryptocurrency, such as Bitcoin, Litecoin, or Potcoin.
APPENDIX B: ADDITIONAL INFORMATION ABOUT IC3 DATA

- Each complaint is reviewed by an IC3 analyst. The analyst categorizes the complaint according to the crime type(s) that are appropriate. Additionally, the analyst will adjust the loss amount if the complaint data does not support the loss amount reported.

- One complaint may have multiple crime types.

- Some complainants may have filed more than once, creating a possible duplicate complaint.

- All location-based reports are generated from information entered when known/provided by the complainant.

- Losses reported in foreign currencies are converted to U.S. dollars when possible.

- Complaint counts represent the number of individual complaints received from each state and do not represent the number of individuals filing a complaint.

- Victim is identified as the individual filing a complaint.

- Subject is identified as the individual perpetrating the scam as reported by the victim.

- “Count by Subject per state” is the number of subjects per state, as reported by victims.

- “Subject earnings per Destination State” is the amount swindled by the subject, as reported by the victim, per state.
Deputy Attorney General Lisa O. Monaco Announces National Cryptocurrency Enforcement Team

Deputy Attorney General Lisa O. Monaco announced today the creation of a National Cryptocurrency Enforcement Team (NCET), to tackle complex investigations and prosecutions of criminal misuses of cryptocurrency, particularly crimes committed by virtual currency exchanges, mixing and tumbling services, and money laundering infrastructure actors. Under the supervision of Assistant Attorney General Kenneth A. Polite Jr., the NCET will combine the expertise of the Department of Justice Criminal Division’s Money Laundering and Asset Recovery Section (MLARS), Computer Crime and Intellectual Property Section (CCIPS) and other sections in the division, with experts detailed from U.S. Attorneys’ Offices. The team will also assist in tracing and recovery of assets lost to fraud and extortion, including cryptocurrency payments to ransomware groups.

“Today we are launching the National Cryptocurrency Enforcement Team to draw on the Department’s cyber and money laundering expertise to strengthen our capacity to dismantle the financial entities that enable criminal actors to flourish — and quite frankly to profit — from abusing cryptocurrency platforms” said Deputy Attorney General Monaco. “As the technology advances, so too must the Department evolve with it so that we’re poised to root out abuse on these platforms and ensure user confidence in these systems.”

“The Criminal Division is already an established leader in investigating and prosecuting the criminal misuse of cryptocurrency,” said Assistant Attorney General Polite. “The creation of this team will build on this leadership by combining and coordinating expertise across the Division in this continuously evolving field to investigate and prosecute the fraudulent misuse, illegal laundering, and other criminal activities involving cryptocurrencies.”

The head of the NCET will report to the Assistant Attorney General in the Criminal Division and will be selected after an application process seeking an individual with experience with complex criminal investigations and prosecutions, as well as the technology underpinning cryptocurrencies and the blockchain. Once selected, the Team Leader will lead the team of attorneys from MLARS, CCIPS, and Assistant U.S. Attorneys (AUSAs) detailed from U.S. Attorneys’ Offices across the country to identify, investigate, support, and pursue cases against cryptocurrency exchanges, infrastructure providers, and other entities that are enabling the misuse of cryptocurrency and related products to commit or facilitate criminal activity.

Importantly, the NCET will draw and build upon the established expertise across the Criminal Division to deter, disrupt, investigate, and prosecute criminal misuse of cryptocurrency, as well as to recover the illicit proceeds of those crimes whenever possible. Because cryptocurrency is used in a wide variety of criminal activity, from being the primary demand mechanism for ransomware payments, to money laundering and the operation of illegal or unregistered money services businesses, to being the preferred means of exchange of value on “dark markets” for illegal drugs, weapons, malware and other hacking tools, the NCET will foster the development of expertise in cryptocurrency and blockchain technologies across all aspects of the Department’s work. The NCET will also play a critical support role for international, federal, state, local, tribal, and territorial law enforcement authorities grappling with these new technologies and new forms of criminal tradecraft.
The NCET builds upon MLARS’s Digital Currency Initiative and will be informed by the Department’s Cryptocurrency Enforcement Framework, released in October 2020. Because crimes involving cryptocurrency can take many forms, the NCET will not only pursue its own cases, but also support existing and future cases brought across the Criminal Division and in the U.S. Attorneys’ Offices across the country.

NCET team members will be drawn from three initial sources: MLARS, CCIPS, and detailees to the Criminal Division from U.S. Attorneys’ Offices across the country. Team members will draw upon the expertise of their home offices while working collaboratively under the Team Leader to combine their expertise in financial systems, blockchain technology, tracing transactions, and applicable criminal statutes to address illegal activity involving cryptocurrency in a structured way. The NCET will:

- Investigate and prosecute cryptocurrency cases, comprising a central part of a nationwide enforcement effort to combat the use of cryptocurrency as an illicit tool.
- Develop strategic priorities for investigations and prosecutions involving cryptocurrency, in consultation with the USAOs, Department components, and investigative agencies involved in cryptocurrency investigations.
- Identify areas for increased investigative and prosecutorial focus, including professional money launderers, ransomware schemes, human traffickers, narcotics traffickers, and financial institutions working with cryptocurrency.
- Build and enhance relationships with cryptocurrency focused AUSAs and prosecutors with other Department litigating components and offices to pursue cryptocurrency investigations and prosecutions.
- Develop and maintain relationships with federal, state, local, and international law enforcement agencies that investigate and prosecute cryptocurrency cases.
- Train and advise federal prosecutors and law enforcement agencies in developing investigative and prosecutorial strategies. Such training and advice will include providing guidance concerning search and seizure warrants, restraining orders, criminal and civil forfeiture allegations, indictments, and other pleadings.
- Support the coordination and sharing of information and evidence among law enforcement offices to maximize the effectiveness of the Department’s investigations, prosecutions, and forfeitures involving cryptocurrency.
- Collaborate and build relationships with private sector actors with expertise in cryptocurrency matters to further the criminal enforcement mission.

The NCET will work closely with other federal agencies, subject matter experts, and its law enforcement partners throughout the government.

**Topic(s):**
Cyber Crime

**Component(s):**
Criminal Division
Office of the Deputy Attorney General

**Press Release Number:**
21-974

*Updated October 6, 2021*
Deputy Attorney General Lisa O. Monaco Announces New Civil Cyber-Fraud Initiative

Deputy Attorney General Lisa O. Monaco announced today the launch of the department’s Civil Cyber-Fraud Initiative, which will combine the department’s expertise in civil fraud enforcement, government procurement and cybersecurity to combat new and emerging cyber threats to the security of sensitive information and critical systems.

“For too long, companies have chosen silence under the mistaken belief that it is less risky to hide a breach than to bring it forward and to report it,” said Deputy Attorney General Monaco. “Well that changes today. We are announcing today that we will use our civil enforcement tools to pursue companies, those who are government contractors who receive federal funds, when they fail to follow required cybersecurity standards — because we know that puts all of us at risk. This is a tool that we have to ensure that taxpayer dollars are used appropriately and guard the public fisc and public trust.”

The creation of the Initiative, which will be led by the Civil Division’s Commercial Litigation Branch, Fraud Section, is a direct result of the department’s ongoing comprehensive cyber review, ordered by Deputy Attorney General Monaco this past May. The review is aimed at developing actionable recommendations to enhance and expand the Justice Department’s efforts against cyber threats.

Civil Cyber-Fraud Initiative Details

The Civil Cyber-Fraud Initiative will utilize the False Claims Act to pursue cybersecurity related fraud by government contractors and grant recipients. The False Claims Act is the government’s primary civil tool to redress false claims for federal funds and property involving government programs and operations. The act includes a unique whistleblower provision, which allows private parties to assist the government in identifying and pursing fraudulent conduct and to share in any recovery and protects whistleblowers who bring these violations and failures from retaliation.

The initiative will hold accountable entities or individuals that put U.S. information or systems at risk by knowingly providing deficient cybersecurity products or services, knowingly misrepresenting their cybersecurity practices or protocols, or knowingly violating obligations to monitor and report cybersecurity incidents and breaches. The benefits of the initiative will include:

- Building broad resiliency against cybersecurity intrusions across the government, the public sector and key industry partners.
- Holding contractors and grantees to their commitments to protect government information and infrastructure.
- Supporting government experts’ efforts to timely identify, create and publicize patches for vulnerabilities in commonly-used information technology products and services.
- Ensuring that companies that follow the rules and invest in meeting cybersecurity requirements are not at a competitive disadvantage.
- Reimbursing the government and the taxpayers for the losses incurred when companies fail to satisfy their cybersecurity obligations.
- Improving overall cybersecurity practices that will benefit the government, private users and the American public.
The department will work closely on the Initiative with other federal agencies, subject matter experts and its law enforcement partners throughout the government.

**Report Cyber-Fraud**

Tips and complaints from all sources about potential cyber-related fraud, waste, abuse and mismanagement can be reported by accessing the webpage of the Civil Division's Fraud Section, which can be found [here](#).

---

**Topic(s):**
Cyber Crime

**Component(s):**
Civil Division
Office of the Deputy Attorney General

**Press Release Number:**
21-971

*Updated October 6, 2021*
Executive Order on Improving the Nation’s Cybersecurity

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Policy. The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people’s security and privacy. The Federal Government must improve its efforts to identify, deter, protect against, detect, and respond to these actions and actors. The Federal Government must also carefully examine what occurred during any major cyber incident and apply lessons learned. But cybersecurity requires more than government action. Protecting our Nation from malicious cyber actors requires the Federal Government to partner with the private sector. The private sector must adapt to the continuously changing threat environment, ensure its products are built and operate securely, and partner with the Federal Government to foster a more secure cyberspace. In the end, the trust we place in our digital infrastructure should be proportional to how trustworthy and transparent that infrastructure is, and to the consequences we will incur if that trust is misplaced.

Incremental improvements will not give us the security we need; instead, the Federal Government needs to make bold changes and significant investments in order to defend the vital institutions that underpin the American way of life. The Federal Government must bring to bear the full scope of its authorities and resources to protect and secure its computer systems, whether they are cloud-based, on-premises, or hybrid. The scope of protection and security must include systems that process data (information technology (IT)) and those that run the vital machinery that ensures our safety (operational technology (OT)).

It is the policy of my Administration that the prevention, detection, assessment, and remediation of cyber incidents is a top priority and essential to national and economic security. The Federal Government must lead by example. All Federal Information Systems should meet or exceed the standards and requirements for cybersecurity set forth in and issued pursuant to this order.
Sec. 2. Removing Barriers to Sharing Threat Information.

(a) The Federal Government contracts with IT and OT service providers to conduct an array of day-to-day functions on Federal Information Systems. These service providers, including cloud service providers, have unique access to and insight into cyber threat and incident information on Federal Information Systems. At the same time, current contract terms or restrictions may limit the sharing of such threat or incident information with executive departments and agencies (agencies) that are responsible for investigating or remediating cyber incidents, such as the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and other elements of the Intelligence Community (IC). Removing these contractual barriers and increasing the sharing of information about such threats, incidents, and risks are necessary steps to accelerating incident deterrence, prevention, and response efforts and to enabling more effective defense of agencies’ systems and of information collected, processed, and maintained by or for the Federal Government.

(b) Within 60 days of the date of this order, the Director of the Office of Management and Budget (OMB), in consultation with the Secretary of Defense, the Attorney General, the Secretary of Homeland Security, and the Director of National Intelligence, shall review the Federal Acquisition Regulation (FAR) and the Defense Federal Acquisition Regulation Supplement contract requirements and language for contracting with IT and OT service providers and recommend updates to such requirements and language to the FAR Council and other appropriate agencies. The recommendations shall include descriptions of contractors to be covered by the proposed contract language.

(c) The recommended contract language and requirements described in subsection (b) of this section shall be designed to ensure that:

(i) service providers collect and preserve data, information, and reporting relevant to cybersecurity event prevention, detection, response, and investigation on all information systems over which they have control, including systems operated on behalf of agencies, consistent with agencies’ requirements;

(ii) service providers share such data, information, and reporting, as they relate to cyber incidents or potential incidents relevant to any agency with which they have contracted, directly with such agency and any other agency that the Director of OMB, in consultation with the Secretary of Defense, the Attorney General, the Secretary of Homeland Security, and the Director of National Intelligence, deems appropriate, consistent with applicable privacy laws, regulations, and policies;

(iii) service providers collaborate with Federal cybersecurity or investigative agencies in their investigations of and responses to incidents or potential incidents on Federal Information Systems, including by implementing technical capabilities, such as monitoring networks for threats in collaboration with agencies they support, as needed; and
(iv) service providers share cyber threat and incident information with agencies, doing so, where possible, in industry-recognized formats for incident response and remediation.

(d) Within 90 days of receipt of the recommendations described in subsection (b) of this section, the FAR Council shall review the proposed contract language and conditions and, as appropriate, shall publish for public comment proposed updates to the FAR.

(e) Within 120 days of the date of this order, the Secretary of Homeland Security and the Director of OMB shall take appropriate steps to ensure to the greatest extent possible that service providers share data with agencies, CISA, and the FBI as may be necessary for the Federal Government to respond to cyber threats, incidents, and risks.

(f) It is the policy of the Federal Government that:

(i) information and communications technology (ICT) service providers entering into contracts with agencies must promptly report to such agencies when they discover a cyber incident involving a software product or service provided to such agencies or involving a support system for a software product or service provided to such agencies;

(ii) ICT service providers must also directly report to CISA whenever they report under subsection (f)(i) of this section to Federal Civilian Executive Branch (FCEB) Agencies, and CISA must centrally collect and manage such information; and

(iii) reports pertaining to National Security Systems, as defined in section 10(h) of this order, must be received and managed by the appropriate agency as to be determined under subsection (g)(i)(E) of this section.

(g) To implement the policy set forth in subsection (f) of this section:

(i) Within 45 days of the date of this order, the Secretary of Homeland Security, in consultation with the Secretary of Defense acting through the Director of the National Security Agency (NSA), the Attorney General, and the Director of OMB, shall recommend to the FAR Council contract language that identifies:

(A) the nature of cyber incidents that require reporting;

(B) the types of information regarding cyber incidents that require reporting to facilitate effective cyber incident response and remediation;

(C) appropriate and effective protections for privacy and civil liberties;

(D) the time periods within which contractors must report cyber incidents based on a graduated scale of severity, with reporting on the most severe cyber incidents not to exceed 3 days after initial detection;

(E) National Security Systems reporting requirements; and

(F) the type of contractors and associated service providers to be covered by the proposed contract language.

(ii) Within 90 days of receipt of the recommendations described in subsection (g)(i) of this section, the FAR Council shall review the recommendations and publish for public comment proposed updates to the FAR.
(iii) Within 90 days of the date of this order, the Secretary of Defense acting through the Director of the NSA, the Attorney General, the Secretary of Homeland Security, and the Director of National Intelligence shall jointly develop procedures for ensuring that cyber incident reports are promptly and appropriately shared among agencies.

(h) Current cybersecurity requirements for unclassified system contracts are largely implemented through agency-specific policies and regulations, including cloud-service cybersecurity requirements. Standardizing common cybersecurity contractual requirements across agencies will streamline and improve compliance for vendors and the Federal Government.

(i) Within 60 days of the date of this order, the Secretary of Homeland Security acting through the Director of CISA, in consultation with the Secretary of Defense acting through the Director of the NSA, the Director of OMB, and the Administrator of General Services, shall review agency-specific cybersecurity requirements that currently exist as a matter of law, policy, or contract and recommend to the FAR Council standardized contract language for appropriate cybersecurity requirements. Such recommendations shall include consideration of the scope of contractors and associated service providers to be covered by the proposed contract language.

(j) Within 60 days of receiving the recommended contract language developed pursuant to subsection (i) of this section, the FAR Council shall review the recommended contract language and publish for public comment proposed updates to the FAR.

(k) Following any updates to the FAR made by the FAR Council after the public comment period described in subsection (j) of this section, agencies shall update their agency-specific cybersecurity requirements to remove any requirements that are duplicative of such FAR updates.

(l) The Director of OMB shall incorporate into the annual budget process a cost analysis of all recommendations developed under this section.

Sec. 3. Modernizing Federal Government Cybersecurity.

(a) To keep pace with today’s dynamic and increasingly sophisticated cyber threat environment, the Federal Government must take decisive steps to modernize its approach to cybersecurity, including by increasing the Federal Government's visibility into threats, while protecting privacy and civil liberties. The Federal Government must adopt security best practices; advance toward Zero Trust Architecture; accelerate movement to secure cloud services, including Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS); centralize and streamline access to cybersecurity data to drive analytics for identifying and managing cybersecurity risks; and invest in both technology and personnel to match these modernization goals.

(b) Within 60 days of the date of this order, the head of each agency shall:
(i) update existing agency plans to prioritize resources for the adoption and use of cloud technology as outlined in relevant OMB guidance;

(ii) develop a plan to implement Zero Trust Architecture, which shall incorporate, as appropriate, the migration steps that the National Institute of Standards and Technology (NIST) within the Department of Commerce has outlined in standards and guidance, describe any such steps that have already been completed, identify activities that will have the most immediate security impact, and include a schedule to implement them; and

(iii) provide a report to the Director of OMB and the Assistant to the President and National Security Advisor (APNSA) discussing the plans required pursuant to subsection (b)(i) and (ii) of this section.

(c) As agencies continue to use cloud technology, they shall do so in a coordinated, deliberate way that allows the Federal Government to prevent, detect, assess, and remediate cyber incidents. To facilitate this approach, the migration to cloud technology shall adopt Zero Trust Architecture, as practicable. The CISA shall modernize its current cybersecurity programs, services, and capabilities to be fully functional with cloud-computing environments with Zero Trust Architecture. The Secretary of Homeland Security acting through the Director of CISA, in consultation with the Administrator of General Services acting through the Federal Risk and Authorization Management Program (FedRAMP) within the General Services Administration, shall develop security principles governing Cloud Service Providers (CSPs) for incorporation into agency modernization efforts. To facilitate this work:

(i) Within 90 days of the date of this order, the Director of OMB, in consultation with the Secretary of Homeland Security acting through the Director of CISA, and the Administrator of General Services acting through FedRAMP, shall develop a Federal cloud-security strategy and provide guidance to agencies accordingly. Such guidance shall seek to ensure that risks to the FCEB from using cloud-based services are broadly understood and effectively addressed, and that FCEB Agencies move closer to Zero Trust Architecture.

(ii) Within 90 days of the date of this order, the Secretary of Homeland Security acting through the Director of CISA, in consultation with the Director of OMB and the Administrator of General Services acting through FedRAMP, shall develop and issue, for the FCEB, cloud-security technical reference architecture documentation that illustrates recommended approaches to cloud migration and data protection for agency data collection and reporting.

(iii) Within 60 days of the date of this order, the Secretary of Homeland Security acting through the Director of CISA shall develop and issue, for FCEB Agencies, a cloud-service governance framework. That framework shall identify a range of services and protections available to agencies based on incident severity. That framework shall also identify data and processing activities associated with those services and protections.

(iv) Within 90 days of the date of this order, the heads of FCEB Agencies, in consultation with the Secretary of Homeland Security acting through the Director of CISA, shall evaluate
the types and sensitivity of their respective agency's unclassified data, and shall provide to the Secretary of Homeland Security through the Director of CISA and to the Director of OMB a report based on such evaluation. The evaluation shall prioritize identification of the unclassified data considered by the agency to be the most sensitive and under the greatest threat, and appropriate processing and storage solutions for those data.

(d) Within 180 days of the date of this order, agencies shall adopt multi-factor authentication and encryption for data at rest and in transit, to the maximum extent consistent with Federal records laws and other applicable laws. To that end:

(i) Heads of FCEB Agencies shall provide reports to the Secretary of Homeland Security through the Director of CISA, the Director of OMB, and the APNSA on their respective agency's progress in adopting multifactor authentication and encryption of data at rest and in transit. Such agencies shall provide such reports every 60 days after the date of this order until the agency has fully adopted, agency-wide, multi-factor authentication and data encryption.

(ii) Based on identified gaps in agency implementation, CISA shall take all appropriate steps to maximize adoption by FCEB Agencies of technologies and processes to implement multifactor authentication and encryption for data at rest and in transit.

(iii) Heads of FCEB Agencies that are unable to fully adopt multi-factor authentication and data encryption within 180 days of the date of this order shall, at the end of the 180-day period, provide a written rationale to the Secretary of Homeland Security through the Director of CISA, the Director of OMB, and the APNSA.

(e) Within 90 days of the date of this order, the Secretary of Homeland Security acting through the Director of CISA, in consultation with the Attorney General, the Director of the FBI, and the Administrator of General Services acting through the Director of FedRAMP, shall establish a framework to collaborate on cybersecurity and incident response activities related to FCEB cloud technology, in order to ensure effective information sharing among agencies and between agencies and CSPs.

(f) Within 60 days of the date of this order, the Administrator of General Services, in consultation with the Director of OMB and the heads of other agencies as the Administrator of General Services deems appropriate, shall begin modernizing FedRAMP by:

(i) establishing a training program to ensure agencies are effectively trained and equipped to manage FedRAMP requests, and providing access to training materials, including videos-on-demand;

(ii) improving communication with CSPs through automation and standardization of messages at each stage of authorization. These communications may include status updates, requirements to complete a vendor's current stage, next steps, and points of contact for questions;

(iii) incorporating automation throughout the lifecycle of FedRAMP, including assessment, authorization, continuous monitoring, and compliance;
(iv) digitizing and streamlining documentation that vendors are required to complete, including through online accessibility and pre-populated forms; and

(v) identifying relevant compliance frameworks, mapping those frameworks onto requirements in the FedRAMP authorization process, and allowing those frameworks to be used as a substitute for the relevant portion of the authorization process, as appropriate.

Sec. 4. Enhancing Software Supply Chain Security.

(a) The security of software used by the Federal Government is vital to the Federal Government’s ability to perform its critical functions. The development of commercial software often lacks transparency, sufficient focus on the ability of the software to resist attack, and adequate controls to prevent tampering by malicious actors. There is a pressing need to implement more rigorous and predictable mechanisms for ensuring that products function securely, and as intended. The security and integrity of “critical software” — software that performs functions critical to trust (such as affording or requiring elevated system privileges or direct access to networking and computing resources) — is a particular concern. Accordingly, the Federal Government must take action to rapidly improve the security and integrity of the software supply chain, with a priority on addressing critical software.

(b) Within 30 days of the date of this order, the Secretary of Commerce acting through the Director of NIST shall solicit input from the Federal Government, private sector, academia, and other appropriate actors to identify existing or develop new standards, tools, and best practices for complying with the standards, procedures, or criteria in subsection (e) of this section. The guidelines shall include criteria that can be used to evaluate software security, include criteria to evaluate the security practices of the developers and suppliers themselves, and identify innovative tools or methods to demonstrate conformance with secure practices.

(c) Within 180 days of the date of this order, the Director of NIST shall publish preliminary guidelines, based on the consultations described in subsection (b) of this section and drawing on existing documents as practicable, for enhancing software supply chain security and meeting the requirements of this section.

(d) Within 360 days of the date of this order, the Director of NIST shall publish additional guidelines that include procedures for periodic review and updating of the guidelines described in subsection (c) of this section.

(e) Within 90 days of publication of the preliminary guidelines pursuant to subsection (c) of this section, the Secretary of Commerce acting through the Director of NIST, in consultation with the heads of such agencies as the Director of NIST deems appropriate, shall issue guidance identifying practices that enhance the security of the software supply chain. Such guidance may incorporate the guidelines published pursuant to subsections (c) and (i) of this section. Such guidance shall include standards, procedures, or criteria regarding:

(i) secure software development environments, including such actions as:
(A) using administratively separate build environments;
(B) auditing trust relationships;
(C) establishing multi-factor, risk-based authentication and conditional access across the enterprise;
(D) documenting and minimizing dependencies on enterprise products that are part of the environments used to develop, build, and edit software;
(E) employing encryption for data; and
(F) monitoring operations and alerts and responding to attempted and actual cyber incidents;

(ii) generating and, when requested by a purchaser, providing artifacts that demonstrate conformance to the processes set forth in subsection (e)(i) of this section;

(iii) employing automated tools, or comparable processes, to maintain trusted source code supply chains, thereby ensuring the integrity of the code;

(iv) employing automated tools, or comparable processes, that check for known and potential vulnerabilities and remediate them, which shall operate regularly, or at a minimum prior to product, version, or update release;

(v) providing, when requested by a purchaser, artifacts of the execution of the tools and processes described in subsection (e)(iii) and (iv) of this section, and making publicly available summary information on completion of these actions, to include a summary description of the risks assessed and mitigated;

(vi) maintaining accurate and up-to-date data, provenance (i.e., origin) of software code or components, and controls on internal and third-party software components, tools, and services present in software development processes, and performing audits and enforcement of these controls on a recurring basis;

(vii) providing a purchaser a Software Bill of Materials (SBOM) for each product directly or by publishing it on a public website;

(viii) participating in a vulnerability disclosure program that includes a reporting and disclosure process;

(ix) attesting to conformity with secure software development practices; and

(x) ensuring and attesting, to the extent practicable, to the integrity and provenance of open source software used within any portion of a product.

(f) Within 60 days of the date of this order, the Secretary of Commerce, in coordination with the Assistant Secretary for Communications and Information and the Administrator of the National Telecommunications and Information Administration, shall publish minimum elements for an SBOM.

(g) Within 45 days of the date of this order, the Secretary of Commerce, acting through the Director of NIST, in consultation with the Secretary of Defense acting through the Director of the NSA, the Secretary of Homeland Security acting through the Director of CISA, the Director
of OMB, and the Director of National Intelligence, shall publish a definition of the term “critical software” for inclusion in the guidance issued pursuant to subsection (e) of this section. That definition shall reflect the level of privilege or access required to function, integration and dependencies with other software, direct access to networking and computing resources, performance of a function critical to trust, and potential for harm if compromised.

(h) Within 30 days of the publication of the definition required by subsection (g) of this section, the Secretary of Homeland Security acting through the Director of CISA, in consultation with the Secretary of Commerce acting through the Director of NIST, shall identify and make available to agencies a list of categories of software and software products in use or in the acquisition process meeting the definition of critical software issued pursuant to subsection (g) of this section.

(i) Within 60 days of the date of this order, the Secretary of Commerce acting through the Director of NIST, in consultation with the Secretary of Homeland Security acting through the Director of CISA and with the Director of OMB, shall publish guidance outlining security measures for critical software as defined in subsection (g) of this section, including applying practices of least privilege, network segmentation, and proper configuration.

(j) Within 30 days of the issuance of the guidance described in subsection (i) of this section, the Director of OMB acting through the Administrator of the Office of Electronic Government within OMB shall take appropriate steps to require that agencies comply with such guidance.

(k) Within 30 days of issuance of the guidance described in subsection (e) of this section, the Director of OMB acting through the Administrator of the Office of Electronic Government within OMB shall take appropriate steps to require that agencies comply with such guidelines with respect to software procured after the date of this order.

(l) Agencies may request an extension for complying with any requirements issued pursuant to subsection (k) of this section. Any such request shall be considered by the Director of OMB on a case-by-case basis, and only if accompanied by a plan for meeting the underlying requirements. The Director of OMB shall on a quarterly basis provide a report to the APNSA identifying and explaining all extensions granted.

(m) Agencies may request a waiver as to any requirements issued pursuant to subsection (k) of this section. Waivers shall be considered by the Director of OMB, in consultation with the APNSA, on a case-by-case basis, and shall be granted only in exceptional circumstances and for limited duration, and only if there is an accompanying plan for mitigating any potential risks.

(n) Within 1 year of the date of this order, the Secretary of Homeland Security, in consultation with the Secretary of Defense, the Attorney General, the Director of OMB, and the Administrator of the Office of Electronic Government within OMB, shall recommend to the FAR Council contract language requiring suppliers of software available for purchase by agencies to comply with, and attest to complying with, any requirements issued pursuant to subsections (g) through (k) of this section.
(o) After receiving the recommendations described in subsection (n) of this section, the FAR Council shall review the recommendations and, as appropriate and consistent with applicable law, amend the FAR.

(p) Following the issuance of any final rule amending the FAR as described in subsection (o) of this section, agencies shall, as appropriate and consistent with applicable law, remove software products that do not meet the requirements of the amended FAR from all indefinite delivery indefinite quantity contracts; Federal Supply Schedules; Federal Government-wide Acquisition Contracts; Blanket Purchase Agreements; and Multiple Award Contracts.

(q) The Director of OMB, acting through the Administrator of the Office of Electronic Government within OMB, shall require agencies employing software developed and procured prior to the date of this order (legacy software) either to comply with any requirements issued pursuant to subsection (k) of this section or to provide a plan outlining actions to remediate or meet those requirements, and shall further require agencies seeking renewals of software contracts, including legacy software, to comply with any requirements issued pursuant to subsection (k) of this section, unless an extension or waiver is granted in accordance with subsection (l) or (m) of this section.

(r) Within 60 days of the date of this order, the Secretary of Commerce acting through the Director of NIST, in consultation with the Secretary of Defense acting through the Director of the NSA, shall publish guidelines recommending minimum standards for vendors’ testing of their software source code, including identifying recommended types of manual or automated testing (such as code review tools, static and dynamic analysis, software composition tools, and penetration testing).

(s) The Secretary of Commerce acting through the Director of NIST, in coordination with representatives of other agencies as the Director of NIST deems appropriate, shall initiate pilot programs informed by existing consumer product labeling programs to educate the public on the security capabilities of Internet-of-Things (IoT) devices and software development practices, and shall consider ways to incentivize manufacturers and developers to participate in these programs.

(t) Within 270 days of the date of this order, the Secretary of Commerce acting through the Director of NIST, in coordination with the Chair of the Federal Trade Commission (FTC) and representatives of other agencies as the Director of NIST deems appropriate, shall identify IoT cybersecurity criteria for a consumer labeling program, and shall consider whether such a consumer labeling program may be operated in conjunction with or modeled after any similar existing government programs consistent with applicable law. The criteria shall reflect increasingly comprehensive levels of testing and assessment that a product may have undergone, and shall use or be compatible with existing labeling schemes that manufacturers use to inform consumers about the security of their products. The Director of NIST shall examine all relevant information, labeling, and incentive programs and employ best practices.
This review shall focus on ease of use for consumers and a determination of what measures can be taken to maximize manufacturer participation.

(u) Within 270 days of the date of this order, the Secretary of Commerce acting through the Director of NIST, in coordination with the Chair of the FTC and representatives from other agencies as the Director of NIST deems appropriate, shall identify secure software development practices or criteria for a consumer software labeling program, and shall consider whether such a consumer software labeling program may be operated in conjunction with or modeled after any similar existing government programs, consistent with applicable law. The criteria shall reflect a baseline level of secure practices, and if practicable, shall reflect increasingly comprehensive levels of testing and assessment that a product may have undergone. The Director of NIST shall examine all relevant information, labeling, and incentive programs, employ best practices, and identify, modify, or develop a recommended label or, if practicable, a tiered software security rating system. This review shall focus on ease of use for consumers and a determination of what measures can be taken to maximize participation.

(v) These pilot programs shall be conducted in a manner consistent with OMB Circular A-119 and NIST Special Publication 2000-02 (Conformity Assessment Considerations for Federal Agencies).

(w) Within 1 year of the date of this order, the Director of NIST shall conduct a review of the pilot programs, consult with the private sector and relevant agencies to assess the effectiveness of the programs, determine what improvements can be made going forward, and submit a summary report to the APNSA.

(x) Within 1 year of the date of this order, the Secretary of Commerce, in consultation with the heads of other agencies as the Secretary of Commerce deems appropriate, shall provide to the President, through the APNSA, a report that reviews the progress made under this section and outlines additional steps needed to secure the software supply chain.

Sec. 5. Establishing a Cyber Safety Review Board.


(b) The Board shall review and assess, with respect to significant cyber incidents (as defined under Presidential Policy Directive 41 of July 26, 2016 (United States Cyber Incident Coordination) (PPD 41)) affecting FCEB Information Systems or non-Federal systems, threat activity, vulnerabilities, mitigation activities, and agency responses.

(c) The Secretary of Homeland Security shall convene the Board following a significant cyber incident triggering the establishment of a Cyber Unified Coordination Group (UCG) as provided by section V(B)(2) of PPD-41; at any time as directed by the President acting through
the APNSA; or at any time the Secretary of Homeland Security deems necessary.

(d) The Board's initial review shall relate to the cyber activities that prompted the establishment of a UCG in December 2020, and the Board shall, within 90 days of the Board's establishment, provide recommendations to the Secretary of Homeland Security for improving cybersecurity and incident response practices, as outlined in subsection (i) of this section.

(e) The Board's membership shall include Federal officials and representatives from private-sector entities. The Board shall comprise representatives of the Department of Defense, the Department of Justice, CISA, the NSA, and the FBI, as well as representatives from appropriate private-sector cybersecurity or software suppliers as determined by the Secretary of Homeland Security. A representative from OMB shall participate in Board activities when an incident under review involves FCEB Information Systems, as determined by the Secretary of Homeland Security. The Secretary of Homeland Security may invite the participation of others on a case-by-case basis depending on the nature of the incident under review.

(f) The Secretary of Homeland Security shall biennially designate a Chair and Deputy Chair of the Board from among the members of the Board, to include one Federal and one private-sector member.

(g) The Board shall protect sensitive law enforcement, operational, business, and other confidential information that has been shared with it, consistent with applicable law.

(h) The Secretary of Homeland Security shall provide to the President through the APNSA any advice, information, or recommendations of the Board for improving cybersecurity and incident response practices and policy upon completion of its review of an applicable incident.

(i) Within 30 days of completion of the initial review described in subsection (d) of this section, the Secretary of Homeland Security shall provide to the President through the APNSA the recommendations of the Board based on the initial review. These recommendations shall describe:

(i) identified gaps in, and options for, the Board's composition or authorities;
(ii) the Board's proposed mission, scope, and responsibilities;
(iii) membership eligibility criteria for private sector representatives;
(iv) Board governance structure including interaction with the executive branch and the Executive Office of the President;
(v) thresholds and criteria for the types of cyber incidents to be evaluated;
(vi) sources of information that should be made available to the Board, consistent with applicable law and policy;
(vii) an approach for protecting the information provided to the Board and securing the cooperation of affected United States individuals and entities for the purpose of the Board's review of incidents; and
(viii) administrative and budgetary considerations required for operation of the Board.
(j) The Secretary of Homeland Security, in consultation with the Attorney General and the APNSA, shall review the recommendations provided to the President through the APNSA pursuant to subsection (i) of this section and take steps to implement them as appropriate.

(k) Unless otherwise directed by the President, the Secretary of Homeland Security shall extend the life of the Board every 2 years as the Secretary of Homeland Security deems appropriate, pursuant to section 871 of the Homeland Security Act of 2002.

Sec. 6. Standardizing the Federal Government’s Playbook for Responding to Cybersecurity Vulnerabilities and Incidents.

(a) The cybersecurity vulnerability and incident response procedures currently used to identify, remediate, and recover from vulnerabilities and incidents affecting their systems vary across agencies, hindering the ability of lead agencies to analyze vulnerabilities and incidents more comprehensively across agencies. Standardized response processes ensure a more coordinated and centralized cataloging of incidents and tracking of agencies’ progress toward successful responses.

(b) Within 120 days of the date of this order, the Secretary of Homeland Security acting through the Director of CISA, in consultation with the Director of OMB, the Federal Chief Information Officers Council, and the Federal Chief Information Security Council, and in coordination with the Secretary of Defense acting through the Director of the NSA, the Attorney General, and the Director of National Intelligence, shall develop a standard set of operational procedures (playbook) to be used in planning and conducting a cybersecurity vulnerability and incident response activity respecting FCEB Information Systems. The playbook shall:

(i) incorporate all appropriate NIST standards;

(ii) be used by FCEB Agencies; and

(iii) articulate progress and completion through all phases of an incident response, while allowing flexibility so it may be used in support of various response activities.

(c) The Director of OMB shall issue guidance on agency use of the playbook.

(d) Agencies with cybersecurity vulnerability or incident response procedures that deviate from the playbook may use such procedures only after consulting with the Director of OMB and the APNSA and demonstrating that these procedures meet or exceed the standards proposed in the playbook.

(e) The Director of CISA, in consultation with the Director of the NSA, shall review and update the playbook annually, and provide information to the Director of OMB for incorporation in guidance updates.

(f) To ensure comprehensiveness of incident response activities and build confidence that unauthorized cyber actors no longer have access to FCEB Information Systems, the playbook shall establish, consistent with applicable law, a requirement that the Director of CISA review
and validate FCEB Agencies’ incident response and remediation results upon an agency’s completion of its incident response. The Director of CISA may recommend use of another agency or a third-party incident response team as appropriate.

(g) To ensure a common understanding of cyber incidents and the cybersecurity status of an agency, the playbook shall define key terms and use such terms consistently with any statutory definitions of those terms, to the extent practicable, thereby providing a shared lexicon among agencies using the playbook.

Sec. 7. Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Networks.

(a) The Federal Government shall employ all appropriate resources and authorities to maximize the early detection of cybersecurity vulnerabilities and incidents on its networks. This approach shall include increasing the Federal Government’s visibility into and detection of cybersecurity vulnerabilities and threats to agency networks in order to bolster the Federal Government’s cybersecurity efforts.

(b) FCEB Agencies shall deploy an Endpoint Detection and Response (EDR) initiative to support proactive detection of cybersecurity incidents within Federal Government infrastructure, active cyber hunting, containment and remediation, and incident response.

(c) Within 30 days of the date of this order, the Secretary of Homeland Security acting through the Director of CISA shall provide to the Director of OMB recommendations on options for implementing an EDR initiative, centrally located to support host-level visibility, attribution, and response regarding FCEB Information Systems.

(d) Within 90 days of receiving the recommendations described in subsection (c) of this section, the Director of OMB, in consultation with Secretary of Homeland Security, shall issue requirements for FCEB Agencies to adopt Federal Government-wide EDR approaches. Those requirements shall support a capability of the Secretary of Homeland Secretary, acting through the Director of CISA, to engage in cyber hunt, detection, and response activities.

(e) The Director of OMB shall work with the Secretary of Homeland Security and agency heads to ensure that agencies have adequate resources to comply with the requirements issued pursuant to subsection (d) of this section.

(f) Defending FCEB Information Systems requires that the Secretary of Homeland Security acting through the Director of CISA have access to agency data that are relevant to a threat and vulnerability analysis, as well as for assessment and threat-hunting purposes. Within 75 days of the date of this order, agencies shall establish or update Memoranda of Agreement (MOA) with CISA for the Continuous Diagnostics and Mitigation Program to ensure object level data, as defined in the MOA, are available and accessible to CISA, consistent with applicable law.

(g) Within 45 days of the date of this order, the Director of the NSA as the National Manager for National Security Systems (National Manager) shall recommend to the Secretary of
Defense, the Director of National Intelligence, and the Committee on National Security Systems (CNSS) appropriate actions for improving detection of cyber incidents affecting National Security Systems, to the extent permitted by applicable law, including recommendations concerning EDR approaches and whether such measures should be operated by agencies or through a centralized service of common concern provided by the National Manager.

(h) Within 90 days of the date of this order, the Secretary of Defense, the Director of National Intelligence, and the CNSS shall review the recommendations submitted under subsection (g) of this section and, as appropriate, establish policies that effectuate those recommendations, consistent with applicable law.

(i) Within 90 days of the date of this order, the Director of CISA shall provide to the Director of OMB and the APNSA a report describing how authorities granted under section 1705 of Public Law 116-283, to conduct threat-hunting activities on FCEB networks without prior authorization from agencies, are being implemented. This report shall also recommend procedures to ensure that mission-critical systems are not disrupted, procedures for notifying system owners of vulnerable government systems, and the range of techniques that can be used during testing of FCEB Information Systems. The Director of CISA shall provide quarterly reports to the APNSA and the Director of OMB regarding actions taken under section 1705 of Public Law 116-283.

(j) To ensure alignment between Department of Defense Information Network (DODIN) directives and FCEB Information Systems directives, the Secretary of Defense and the Secretary of Homeland Security, in consultation with the Director of OMB, shall:

(i) within 60 days of the date of this order, establish procedures for the Department of Defense and the Department of Homeland Security to immediately share with each other Department of Defense Incident Response Orders or Department of Homeland Security Emergency Directives and Binding Operational Directives applying to their respective information networks;

(ii) evaluate whether to adopt any guidance contained in an Order or Directive issued by the other Department, consistent with regulations concerning sharing of classified information; and

(iii) within 7 days of receiving notice of an Order or Directive issued pursuant to the procedures established under subsection (j)(i) of this section, notify the APNSA and Administrator of the Office of Electronic Government within OMB of the evaluation described in subsection (j)(ii) of this section, including a determination whether to adopt guidance issued by the other Department, the rationale for that determination, and a timeline for application of the directive, if applicable.
Sec. 8. Improving the Federal Government’s Investigative and Remediation Capabilities.

(a) Information from network and system logs on Federal Information Systems (for both on-premises systems and connections hosted by third parties, such as CSPs) is invaluable for both investigation and remediation purposes. It is essential that agencies and their IT service providers collect and maintain such data and, when necessary to address a cyber incident on FCEB Information Systems, provide them upon request to the Secretary of Homeland Security through the Director of CISA and to the FBI, consistent with applicable law.

(b) Within 14 days of the date of this order, the Secretary of Homeland Security, in consultation with the Attorney General and the Administrator of the Office of Electronic Government within OMB, shall provide to the Director of OMB recommendations on requirements for logging events and retaining other relevant data within an agency’s systems and networks. Such recommendations shall include the types of logs to be maintained, the time periods to retain the logs and other relevant data, the time periods for agencies to enable recommended logging and security requirements, and how to protect logs. Logs shall be protected by cryptographic methods to ensure integrity once collected and periodically verified against the hashes throughout their retention. Data shall be retained in a manner consistent with all applicable privacy laws and regulations. Such recommendations shall also be considered by the FAR Council when promulgating rules pursuant to section 2 of this order.

(c) Within 90 days of receiving the recommendations described in subsection (b) of this section, the Director of OMB, in consultation with the Secretary of Commerce and the Secretary of Homeland Security, shall formulate policies for agencies to establish requirements for logging, log retention, and log management, which shall ensure centralized access and visibility for the highest level security operations center of each agency.

(d) The Director of OMB shall work with agency heads to ensure that agencies have adequate resources to comply with the requirements identified in subsection (c) of this section.

(e) To address cyber risks or incidents, including potential cyber risks or incidents, the proposed recommendations issued pursuant to subsection (b) of this section shall include requirements to ensure that, upon request, agencies provide logs to the Secretary of Homeland Security through the Director of CISA and to the FBI, consistent with applicable law. These requirements should be designed to permit agencies to share log information, as needed and appropriate, with other Federal agencies for cyber risks or incidents.


(a) Within 60 days of the date of this order, the Secretary of Defense acting through the National Manager, in coordination with the Director of National Intelligence and the CNSS, and in consultation with the APNSA, shall adopt National Security Systems requirements that are equivalent to or exceed the cybersecurity requirements set forth in this order that are
otherwise not applicable to National Security Systems. Such requirements may provide for exceptions in circumstances necessitated by unique mission needs. Such requirements shall be codified in a National Security Memorandum (NSM). Until such time as that NSM is issued, programs, standards, or requirements established pursuant to this order shall not apply with respect to National Security Systems.

(b) Nothing in this order shall alter the authority of the National Manager with respect to National Security Systems as defined in National Security Directive 42 of July 5, 1990 (National Policy for the Security of National Security Telecommunications and Information Systems) (NSD-42). The FCEB network shall continue to be within the authority of the Secretary of Homeland Security acting through the Director of CISA.

Sec. 10. Definitions. For purposes of this order:

(a) the term “agency” has the meaning ascribed to it under 44 U.S.C. 3502.

(b) the term “auditing trust relationship” means an agreed-upon relationship between two or more system elements that is governed by criteria for secure interaction, behavior, and outcomes relative to the protection of assets.

(c) the term “cyber incident” has the meaning ascribed to an “incident” under 44 U.S.C. 3552(b)(2).

(d) the term “Federal Civilian Executive Branch Agencies” or “FCEB Agencies” includes all agencies except for the Department of Defense and agencies in the Intelligence Community.

(e) the term “Federal Civilian Executive Branch Information Systems” or “FCEB Information Systems” means those information systems operated by Federal Civilian Executive Branch Agencies, but excludes National Security Systems.

(f) the term “Federal Information Systems” means an information system used or operated by an agency or by a contractor of an agency or by another organization on behalf of an agency, including FCEB Information Systems and National Security Systems.

(g) the term “Intelligence Community” or “IC” has the meaning ascribed to it under 50 U.S.C. 3003(4).

(h) the term “National Security Systems” means information systems as defined in 44 U.S.C. 3552(b)(6), 3553(e)(2), and 3553(e)(3).

(i) the term “logs” means records of the events occurring within an organization's systems and networks. Logs are composed of log entries, and each entry contains information related to a specific event that has occurred within a system or network.

(j) the term “Software Bill of Materials” or “SBOM” means a formal record containing the details and supply chain relationships of various components used in building software. Software developers and vendors often create products by assembling existing open source and commercial software components. The SBOM enumerates these components in a product. It is analogous to a list of ingredients on food packaging. An SBOM is useful to those who
develop or manufacture software, those who select or purchase software, and those who operate software. Developers often use available open source and third-party software components to create a product; an SBOM allows the builder to make sure those components are up to date and to respond quickly to new vulnerabilities. Buyers can use an SBOM to perform vulnerability or license analysis, both of which can be used to evaluate risk in a product. Those who operate software can use SBOMs to quickly and easily determine whether they are at potential risk of a newly discovered vulnerability. A widely used, machine-readable SBOM format allows for greater benefits through automation and tool integration. The SBOMs gain greater value when collectively stored in a repository that can be easily queried by other applications and systems. Understanding the supply chain of software, obtaining an SBOM, and using it to analyze known vulnerabilities are crucial in managing risk.

(k) the term “Zero Trust Architecture” means a security model, a set of system design principles, and a coordinated cybersecurity and system management strategy based on an acknowledgement that threats exist both inside and outside traditional network boundaries. The Zero Trust security model eliminates implicit trust in any one element, node, or service and instead requires continuous verification of the operational picture via real-time information from multiple sources to determine access and other system responses. In essence, a Zero Trust Architecture allows users full access but only to the bare minimum they need to perform their jobs. If a device is compromised, zero trust can ensure that the damage is contained. The Zero Trust Architecture security model assumes that a breach is inevitable or has likely already occurred, so it constantly limits access to only what is needed and looks for anomalous or malicious activity. Zero Trust Architecture embeds comprehensive security monitoring; granular risk-based access controls; and system security automation in a coordinated manner throughout all aspects of the infrastructure in order to focus on protecting data in real-time within a dynamic threat environment. This data-centric security model allows the concept of least-privileged access to be applied for every access decision, where the answers to the questions of who, what, when, where, and how are critical for appropriately allowing or denying access to resources based on the combination of sever.

Sec. 11. General Provisions.

(a) Upon the appointment of the National Cyber Director (NCD) and the establishment of the related Office within the Executive Office of the President, pursuant to section 1752 of Public Law 116-283, portions of this order may be modified to enable the NCD to fully execute its duties and responsibilities.

(b) Nothing in this order shall be construed to impair or otherwise affect:

(i) the authority granted by law to an executive department or agency, or the head thereof; or

(ii) the functions of the Director of the Office of Management and Budget relating to
budgetary, administrative, or legislative proposals.

(c) This order shall be implemented in a manner consistent with applicable law and subject to the availability of appropriations.

(d) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

(e) Nothing in this order confers authority to interfere with or to direct a criminal or national security investigation, arrest, search, seizure, or disruption operation or to alter a legal restriction that requires an agency to protect information learned in the course of a criminal or national security investigation.

JOSEPH R. BIDEN JR.

THE WHITE HOUSE,
May 12, 2021.
FBI Strategy Addresses Evolving Cyber Threat

Director Wray Emphasizes Closer Partnerships to Combat Cyber Threats and Impose Greater Costs to Cyber Actors

FBI Director Christopher Wray announced the Bureau’s new strategy for countering cyber threats in remarks at the National Cybersecurity Summit today.

The strategy, Wray explained, is to “impose risk and consequences on cyber adversaries”—making it harder for both cyber criminals and foreign governments to use malicious cyber activity to achieve their objectives.

“We’ve got to change the cost-benefit calculus of criminals and nation-states who believe they can compromise U.S. networks, steal U.S. financial and intellectual property, and hold our critical infrastructure at risk, all without incurring any risk themselves,” he said.

The centerpiece of the new strategy is the role the FBI plays as an “indispensable partner” to federal counterparts, foreign partners, and private-sector partners. “We want to make sure we’re doing everything we can to help our partners do what they need to do,” said Wray. “That means using our role as the lead federal agency with law enforcement and intelligence responsibilities to not only pursue our own actions, but to enable our partners to defend networks, attribute malicious activity, impose sanctions for bad behavior, and take the fight to our adversaries overseas.”

The strategy recognizes that no single agency—or even government—can combat cyber threats alone, and that when possible, actions by the FBI and its partners will be sequenced for maximum impact.

Wray’s remarks helped close out the first in a series of four events hosted by the Cybersecurity and Infrastructure Security Agency, or CISA. The summit seeks to bring together cyber leaders from government, academia, and industry.

This government effort to sequence unilateral, joint, and enabled operations against cyber adversaries is coordinated by the National Cyber Investigative Joint Task Force. Led by the FBI, the task force includes more than 30 co-located agencies from the Intelligence Community and law enforcement and is focused on the most significant threats.

The collaboration envisioned in the FBI cyber strategy leverages the skills of multiple agencies as well as the insights of industry, nonprofit, and academic institutions. An effective threat response must involve every part of society that is affected by malicious cyber activity and every part of society that can help hold the line against it.

Wray said that the most significant current threats are coming from the Chinese government targeting our intellectual property, Russian efforts to undermine our critical infrastructure, and increasingly sophisticated criminal cyber syndicates that seek to steal from individuals and institutions.

To combat these evolving threats, the FBI leverages its broad domestic and international presence, with cyber squads in every FBI field office and rapid response teams ready to respond to major incidents wherever and whenever they happen.

The cyber strategy announced by Director Wray builds on more than a century of innovation by the FBI to adapt to and confront threats to the American people.

Resources
- CISA Cybersecurity Summit: Addressing Threats Through Partnerships
- Cyber Crime

Videos
- Director Wray Addresses CISA Cybersecurity Summit

“We want to make sure we’re doing everything we can to help our partners do what they need to do.”

FBI Director Christopher Wray

The FBI Cyber Strategy
The FBI’s cyber strategy is to impose risk and consequences on cyber adversaries through our unique authorities, our world-class capabilities, and our enduring partnerships.

Learn more (pdf)
FinCEN Announces $100 Million Enforcement Action Against Unregistered Futures Commission Merchant BitMEX for Willful Violations of the Bank Secrecy Act

Contact: Office of Strategic Communications, 703-905-3770
Immediate Release: August 10, 2021

WASHINGTON—The Financial Crimes Enforcement Network (FinCEN) has assessed a civil money penalty (https://www.fincen.gov/sites/default/files/enforcement_action/2021-08-10/Assessment_BITMEX_508_FINAL.pdf) in the amount of $100 million against BitMEX, one of the oldest and largest convertible virtual currency derivatives exchanges, for violations of the Bank Secrecy Act (BSA) and FinCEN’s implementing regulations.

BitMEX, which operated as an unregistered futures commission merchant (FCM) and provided money transmission services, willfully failed to comply with its obligations under the BSA. FinCEN’s action is part of a global settlement with the U.S. Commodity Futures Trading Commission (CFTC).

“BitMEX’s rapid growth into one of the largest futures commission merchants offering convertible virtual currency derivatives without a commensurate anti-money laundering program put the U.S. financial system at meaningful risk,” FinCEN’s Deputy Director Annalou Tirol said. “It is critical that platforms build in financial integrity from the start, so that financial innovation and opportunity are protected from vulnerabilities and exploitation.”

For over 6 years, BitMEX failed to implement and maintain a compliant anti-money laundering program and a customer identification program, and it failed to report certain suspicious activity. These willful failures expose financial institutions to an increased risk of conducting transactions with money launderers and terrorist financiers, including noncompliant exchanges in high-risk jurisdictions, ransomware attackers, and darknet marketplaces. BitMEX conducted at least $209 million worth of transactions with known darknet markets or unregistered money services businesses providing mixing services. BitMEX also conducted transactions involving high-risk jurisdictions and alleged fraud schemes. BitMEX failed to file a Suspicious Activity Report (SAR) on at least 588 specific suspicious transactions.

From approximately 2014 through 2020, BitMEX allowed customers to access its platform and conduct derivative trading without appropriate customer due diligence – collecting only an email address and failing to verify customer identity. Despite BitMEX’s public representation that its platform was not conducting business with U.S. persons, FinCEN found that BitMEX failed to implement appropriate policies, procedures, and internal controls to screen for customers that use a virtual private network to access the trading platform and circumvent internet protocol monitoring. In some instances, BitMEX senior leadership altered U.S. customer information to hide the customer’s true location.
In addition to paying a civil money penalty, BitMEX has agreed to engage an independent consultant to conduct a historical analysis of its transaction data, sometimes referred to as a “SAR lookback,” to determine whether BitMEX must file additional SARs on this activity. BitMEX will also engage an independent consultant to conduct two reviews, including relevant testing, to ensure that appropriate policies, procedures, and controls are in place that are effective and reasonably designed and implemented to ensure that BitMEX is not operating wholly or in substantial part in the United States.

This is FinCEN’s first enforcement action against an FCM. FinCEN appreciates the close collaboration with its partners at the CFTC on this matter. The CFTC and BitMEX have separately agreed to a Consent Order (https://www.cftc.gov/PressRoom/PressReleases/8412-21) requiring the payment of a civil money penalty with additional equitable relief. FinCEN’s $100 million assessment will be satisfied by immediate payments totaling $80 million to FinCEN and the CFTC, with $20 million suspended pending the successful completion of the SAR lookback and independent consultant reviews.
FTC Strengthens Security Safeguards for Consumer Financial Information Following Widespread Data Breaches

October 27, 2021

Agency updates Safeguards Rule to better protect the American public from breaches and cyberattacks that lead to identity theft and other financial losses

FOR RELEASE


The Federal Trade Commission today announced a newly updated rule that strengthens the data security safeguards that financial institutions are required to put in place to protect their customers’ financial information. In recent years, widespread data breaches and cyberattacks have resulted in significant harms to consumers, including monetary loss, identity theft, and other forms of financial distress. The FTC’s updated Safeguards Rule requires non-banking financial institutions, such as mortgage brokers, motor vehicle dealers, and payday lenders, to develop, implement, and maintain a comprehensive security system to keep their customers’ information safe.

“If financial institutions and other entities that collect sensitive consumer data have a responsibility to protect it,” said Samuel Levine, Director of the FTC’s Bureau of Consumer Protection. “The updates adopted by the Commission to the Safeguards Rule detail common-sense steps that these institutions must implement to protect consumer data from cyberattacks and other threats.”

The changes adopted by the Commission to the Safeguards Rule include more specific criteria for what safeguards financial institutions must implement as part of their information security program such as limiting who can access consumer data and using encryption to secure the data. Under the updated Safeguards Rule, institutions must also explain their information sharing practices, specifically the administrative, technical, and physical safeguards the financial institutions use to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle customers’ secure information. In addition, financial institutions will be required to designate a single qualified
individual to oversee their information security program and report periodically to an organization’s board of directors, or a senior officer in charge of information security.

The Safeguards Rule was mandated by Congress under the 1999 Gramm-Leach-Bliley Act. Today’s updates are the result of years of public input. In 2019, the FTC sought comment on proposed changes to the Safeguards Rule and, in 2020 held a public workshop on the Safeguards Rule.

In addition to the updates, the FTC is seeking comment on whether to make an additional change to the Safeguards Rule to require financial institutions to report certain data breaches and other security events to the Commission. The FTC is issuing a supplemental notice of proposed rulemaking, which will be published in the Federal Register shortly. The public will have 60 days after the notice is published in the Federal Register to submit a comment.

Today, the FTC also announced it adopted largely technical changes to its authority under a separate Gramm-Leach Bliley Act rule, which requires financial institutions to inform customers about their information-sharing practices and allow customers to opt out of having their information shared with certain third parties. These changes align the rule with changes made under the 2010 Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank). Under Dodd-Frank, Congress narrowed the FTC’s jurisdiction under that rule to only apply to motor vehicle dealers.

The Commission voted 5-0 to publish the final revisions to update the FTC’s jurisdiction under Dodd-Frank and the supplemental notice of proposed rulemaking to the Safeguards Rule in the Federal Register. The Commission voted 3-2 to publish the revisions to the Safeguards Rule in the Federal Register. Commissioners Noah Joshua Phillips and Christine S. Wilson voted no and issued a joint dissenting statement. Chair Lina M. Khan and Rebecca Kelly Slaughter issued a separate joint statement.

The Federal Trade Commission works to promote competition, stop deceptive and unfair business practices and scams, and educate consumers. Report fraud, scams, or bad business practices at ReportFraud.ftc.gov. Get consumer advice at consumer.ftc.gov. Also, follow the FTC on social media, subscribe to press releases, and read the FTC’s blogs.

PRESS RELEASE REFERENCE:
FTC Extends Comment Deadline on Proposed Changes to Safeguards Rule
FTC Seeks Comment on Proposed Amendments to Safeguards and Privacy Rules
FTC to Host Workshop Examining Issues Related to Proposed Amendments to the Safeguards Rule
FTC Safeguards Workshop Postponed Until July 13, 2020. Will be Held Online
FTC Releases Agenda for Safeguards Rule Virtual Workshop
FTC to Host Virtual Workshop July 13 on Proposed Changes to Safeguards Rule

Contact Information

MEDIA CONTACT:
Juliana Gruenwald Henderson
Office of Public Affairs
202-326-2924

STAFF CONTACT:
David Lincicum
Bureau of Consumer Protection
202-326-2773
338 F.R.D. 7
United States District Court, District of Columbia.

GUO WENGUI, Plaintiff,
v.
CLARK HILL, PLC, et al., Defendants.

Civil Action No. 19-3195 (JEB)
Signed 01/12/2021

Synopsis
Background: Client, who brought action for legal malpractice, breach of fiduciary duty, and breach of contract against his former law firm, after hacking incident at firm resulted in release of his confidential information on the Internet, moved to compel production of report produced by external security-consulting firm, as well as mandate to compel firm to provide more complete answers to interrogatories.

Holdings: The District Court, James E. Boasberg, J., held that:

[1] report was not protected by work-product doctrine;

[2] report was not protected by attorney-client privilege; and

[3] information relating to effect of cyberattack on firm's other clients was relevant to client's action.

Motion granted.

Procedural Posture(s): Motion to Compel Discovery.

West Headnotes (13)

Privileged Communications and Confidentiality ⇔ Presumptions and burden of proof
The party seeking to withhold a document under either the work-product doctrine or the attorney-client privilege bears the burden of showing that the privilege applies. Fed. R. Civ. P. 26(b)(3)(A), 33(a)(2), 34(a).

To determine whether a document was prepared in anticipation of litigation for purposes of a work-product privilege analysis, courts apply the “because of test,” asking whether, in light of the nature of the document and the factual situation in the particular case, the document can fairly be said to have been prepared or obtained because of the prospect of litigation. Fed. R. Civ. P. 26(b)(3)(A).

Where a document would have been created in substantially similar form regardless of the litigation, it fails the “because of” test, meaning that work product protection is not available. Fed. R. Civ. P. 26(b)(3)(A).

The work-product privilege has no applicability to documents prepared by lawyers in the ordinary course of business or for other nonlitigation purposes. Fed. R. Civ. P. 26(b)(3)(A).

Report prepared by external security-consulting firm, that was hired by law firm after hacking incident at firm, was not protected by work-product privilege in action for legal malpractice, breach of fiduciary duty, and breach of contract brought by former client whose confidential information was released on Internet; firm did not meet its burden to show that report, or substantially similar document, would not have been created in ordinary course of...
business irrespective of litigation, discovering how breach occurred was necessary business function regardless of litigation or regulatory inquiries, and fact that report was used for range of non-litigation purposes reinforced notion that it could not be fairly described as prepared in anticipation of litigation. Fed. R. Civ. P. 26(b)(3) (A).

1 Cases that cite this headnote

[6] Privileged Communications and Confidentiality ➔ Elements in general; definition

Privileged Communications and Confidentiality ➔ Distinguished from work product

Distinct from the work-product privilege, the “attorney-client privilege” protects a confidential communication between attorney and client if that communication was made for the purpose of obtaining or providing legal advice to the client.

[7] Privileged Communications and Confidentiality ➔ Communications Through or in Presence or Hearing of Others; Communications with Third Parties

The attorney-client privilege can attach to reports of third parties made at the request of the attorney or the client where the purpose of the report was to put in usable form information obtained from the client.

[8] Privileged Communications and Confidentiality ➔ Communications Through or in Presence or Hearing of Others; Communications with Third Parties

The “Kovel doctrine,” under which attorney-client privilege can attach to reports of third parties made at request of attorney or client where the purpose of the report was to put in usable form information obtained from client, must be applied narrowly lest the attorney-client privilege be construed to engulf all manner of services that should not be summarily excluded from the adversary process.

[9] Privileged Communications and Confidentiality ➔ Distinguished from work product

Privileged Communications and Confidentiality ➔ Absolute or qualified privilege

Unlike work-product privilege, which may be overcome by sufficient showing of need, attorney-client privilege is absolute.

[10] Privileged Communications and Confidentiality ➔ Experts and professionals in general

Report prepared by external security-consulting firm, that was hired by law firm after hacking incident at firm, was not protected by attorney-client privilege in action for legal malpractice, breach of fiduciary duty, and breach of contract brought by former client whose confidential information was released on Internet; firm's true objective was gleaning expertise in cybersecurity, not in obtaining legal advice from its outside counsel, report was shared with both staff and FBI, presumably with an eye toward facilitating both entities’ further efforts at investigation and remediation, external security-consulting firm was engaged for immediate incident response and began its work as attack was thought to still be ongoing, and report included pages of specific remediation advice.


Federal Civil Procedure ➔ Particular Subject Matters

Information relating to effect of cyberattack on law firm’s other clients was relevant to former client's action for legal malpractice, breach of fiduciary duty, and breach of contract arising from release of his confidential information on Internet, and any concerns
about attorney-client **privilege** in regard to other clients could be safeguarded with appropriate redactions in responsive documents, and with tailored interrogatory answers, and thus information was discoverable; scope of attack was directly germane to central issue in case, namely, sufficiency and reasonableness of firm's cybersecurity. Fed. R. Civ. P. 26(b)(1), 33(a)(2), 34(a).

[12] **Privileged Communications and Confidentiality**  
Client information; retain and authority  
Under the general rule, the attorney-client **privilege** does not protect from disclosure the identity of the client and the general purpose of the work performed.

[13] **Privileged Communications and Confidentiality**  
Client information; retain and authority  
When a client's identity is sufficiently intertwined with the client's confidences, the attorney-client **privilege** applies.

**Attorneys and Law Firms**

*9 Ari Scott Casper, The Casper Firm, LLC, Baltimore, MD, for Plaintiff.

Kali N. Bracey, Jessica Ring Amunson, Jenner & Block LLP, Washington, DC, David P. Saunders, Pro Hac Vice, John R. Storino, Leigh J. Jahnig, Jenner & Block LLP, Chicago, IL, for Defendants.

**MEMORANDUM OPINION**

JAMES E. BOASBERG, United States District Judge

Malicious cyberattacks have unfortunately become a routine part of our modern digital world. So have the lawsuits that follow them, alleging, as this one does, that the hacked institution failed to take sufficient precautions to protect the plaintiff's data. During such litigation, disputes frequently arise over whether documents generated by the defendant in the wake of a data breach — e.g., forensic reports, analyses, and internal communications — are privileged or instead must be turned over in discovery. See, e.g., *In re Dominion Dental Servs. USA, Inc. Data Breach Litig.*, 429 F. Supp. 3d 190, 193–94 (E.D. Va. 2019) (citing cases). This Court now adds its thoughts to the accumulating caselaw.

Plaintiff Guo Wengui has moved to compel Defendant Clark Hill, PLC, his former law firm, to produce “all reports of its forensic investigation into the cyberattack” that led to the public dissemination of Mr. Guo's confidential information. See ECF No. 25-1 (Mot.) at 3; see generally *Guo Wengui v. Clark Hill, PLC*, 440 F. Supp. 3d 30 (D.D.C. 2020) (discussing Plaintiff's allegations). He also asks that the Court mandate that Defendant provide more complete answers to certain interrogatories regarding its investigation into the hack. See Mot. at 3.

Clark Hill rejoins that it has turned over all relevant internally generated materials and that the other documents Plaintiff seeks, which were produced by external security-consulting firm Duff & Phelps, are covered by both the attorney-client and work-product **privileges**. See ECF No. 30-1 (Opp.) at 2. The firm also refuses to answer Plaintiff's interrogatories seeking “Clark Hill's understanding of the facts or reasons why” the attack occurred, claiming that “its ‘understanding’ of the progression of the ... incident is based solely on the advice of outside counsel and consultants retained by outside counsel” and is therefore privileged. See ECF No. 29-4 (Defendant's Third Supplemental Interrogatory Responses) at 13–14; see also id., at 19 (declining to answer interrogatory regarding effect of attack “to the extent it calls for knowledge that Clark Hill obtained as a result of its consultations with outside counsel and consultants retained by outside counsel”).

Separately, Clark Hill also maintains that it cannot respond to Guo's additional requests for “information or documents related to [its] clients other than Plaintiff” who may (or may not) have been affected by the hack at issue, on the grounds that such information is both irrelevant and privileged. See Opp. at 22–24.
I. Legal Standard

1. Work-Product Privilege

Rule 26 codifies what is known as the work-product privilege, under which, “[o]ordinarily, a party may not discover documents and tangible things that are prepared in anticipation of litigation ... by or for another party or its representative (including the other party's attorney, consultant, ... or agent).” Fed R. Civ. P. 26(b)(3)(A). To determine whether a document was “prepared in anticipation of litigation,” courts in this circuit apply the “because of” test, asking “whether, in light of the nature of the document and the factual situation in the particular case, the document can fairly be said to have been prepared or obtained because of the prospect of litigation.” United States v. Deloitte LLP, 610 F.3d 129, 137 (D.C. Cir. 2010) (emphasis added) (citation omitted). “Where a document would have been created ‘in substantially similar form’ regardless of the litigation,” it fails that test, meaning that “work product protection is not available.” FTC v. Boehringer Ingelheim Pharms., Inc., 778 F.3d 142, 149 (D.C. Cir. 2015) (quoting Deloitte, 610 F.3d at 138). For that reason, “the privilege has no applicability to documents prepared by lawyers in the ordinary course of business for or other nonlitigation purposes.” In re Sealed Case, 146 F.3d 881, 887 (D.C. Cir. 1998) (citation and internal quotation marks omitted); see also Banneker Ventures, LLC v. Graham, 253 F. Supp. 3d 64, 72 (D.D.C. 2017) (“Documents that would have been created in the ordinary course of business irrespective of litigation are not protected by the work-product doctrine.”) (cleaned up); United States v. Adlman, 134 F.3d 1194, 1204 (2d Cir. 1998) (“If the district court concludes that substantially the same [document] would have been prepared in any event — as part of the ordinary course of business ... — then the court should conclude [it] was not prepared because of ... litigation.”).

2. [3] [4] In light of the record before the Court, including the Duff & Phelps Report itself (which the Court has reviewed in camera), Clark Hill has not met its burden to show that the Report, or a substantially similar document, “would [not] have been created in the ordinary course of business irrespective of litigation.” Banneker Ventures, 253 F. Supp. 3d at 72. For many organizations, surely among them law firms that handle sensitive materials, “discovering how [a cyber] breach occurred [is] a necessary business function regardless of litigation or regulatory inquiries. [There is a] need[ ] to conduct an investigation ... in order to figure out the problem that allowed the breach to occur so that [the organization] [can] solve that problem and ensure such a breach [cannot] happen again.” *11 Dominion Dental, 429 F. Supp. 3d at 193 (quoting In re Premera Blue Cross Customer Data Sec. Breach Litig. (Premera I), 296 F. Supp. 3d 1230, 1245–
46 (D. Or. 2017)). It is therefore more likely than not, if not “highly likely[,] that [Clark Hill] would have conducted [an] investigation” into the attack's cause, nature, and effect “irrespective of the prospect of litigation.” ISS Marine Servs., 905 F. Supp. 2d at 137. From the Court’s in camera review, it is clear that the Duff & Phelps Report summarizes the findings of such an investigation, and that “substantially the same [document] would have been prepared in any event ... as part of the ordinary course of [Defendant's] business.” Adlman, 134 F.3d at 1204.

Defendant, notably, does not seem to quarrel with this general thesis. Instead, it offers a more nuanced position, arguing that the Report qualifies as being prepared in anticipation of litigation because it was the result of only one half of a “two-tracked investigation of the incident.” Opp. at 2. On one track, Clark Hill’s usual cybersecurity vendor, called eSentire, worked “to investigate and remediate the attack” so as to preserve “business continuity.” Id.; see also id. at 5 (“Over the ... several weeks [after the attack], Clark Hill engaged with ... eSentire ... to ascertain the nature and remediate the effects of the attack.”). Clark Hill points out that it has disclosed documents related to eSentire’s work. Id. at 2. On a “separate track from the eSentire work,” Defendant insists, was Duff & Phelps, retained by MPG “for the sole purpose of assisting [the firm] in gathering information necessary to render timely legal advice.” ECF No. 29-17 (Engagement Letter from MPG) at 1; see also ECF No. 29-16 (Engagement Letter from Duff & Phelps) at ECF p. 1.

In other words, Clark Hill claims, citing In re Target Corp. Customer Data Sec. Breach Litig., MDL No. 14-2522, 2015 WL 6777384, at *2–3 (D. Minn. Oct. 23, 2015), that it had one “ordinary-course investigation” by eSentire “set up so that [it] could learn how the breach happened and ... respond to it appropriately” — which did not result in protected work product — while it also engaged a “separate team” to “inform[ ] [its] counsel about the breach so that [they] could provide ... legal advice and prepare to defend the company in litigation.” Id. (finding “information generated along [the latter] track” to be protected work product). Under the Target court’s approach, the latter investigation and report would apparently not have existed but for the prospect of litigation, even as the other report would have been prepared “in the ordinary course of business.” In re Sealed Case, 146 F.3d at 887 (citation omitted). Ergo, says Clark Hill, it has appropriately disclosed eSentire’s work and held on to Duff & Phelps’s.

The problem for the defense here is that its two-track story finds little support in the record. The firm offers no sworn statement averring that eSentire conducted a separate “investigation” with the purpose of “learn[ing] how the breach happened” or facilitating an “appropriate[ ]” response. Target, 2015 WL 6777384, at *2. The closest it comes is an equivocal statement by Eric Rousseau, its Director of Information Security, that “[b]ecause of eSentire's work, Clark Hill did not need the Duff & Phelps report for business continuity.” ECF No. 29-29 (Declaration of Eric Rousseau), ¶ 4. That is not the same as stating that eSentire conducted its own inquiry to (in the words of Defendant’s brief) help Clark Hill “ascertain the nature and remedy the effects of the attack.” Opp. at 5. On the contrary, Defendant’s own interrogatory answers state that “its understanding of the progression of the September 12, 2017 cyber-incident is based solely on the advice of outside counsel and consultants retained by outside counsel.” Def.’s 3d Suppl. Interrog. Resps. at 13–14 (emphasis added) (internal quotation marks omitted); see also ECF No. 25-6 (Defendant’s Second Supplemental Interrogatory Responses) at 17–18 (earlier interrogatory answer stating that “any belief held by Clark Hill regarding the cause or origination of the cyber-incident is the result of discussions with outside counsel and consultants retained by outside counsel!”) (emphasis added). Consistent with those answers, there is no evidence that eSentire ever produced any findings, let alone a comprehensive report like the one produced by Duff & Phelps, about “the problem that allowed the breach to occur” or any recommendations to “ensure *12 such a breach [cannot] happen again.” In re Premera Blue Cross Customer Data Sec. Breach Litig. (Premera II), 329 F.R.D. 656, 666 (D. Or. 2019); see also Premera I, 296 F. Supp. 3d at 1245 (“This situation is unlike the Target data breach case .... [There,] the company performed its own independent data breach investigation that was produced in discovery.”) (emphasis added); Dominion Dental, 429 F. Supp. 3d at 195 (“Here, defendants have presented no evidence of a two-track investigation. The ... report [at issue] appears to be the only report commissioned by defendants in connection with the data breach at issue.”).

The record instead suggests that on September 14, 2017, two days after the cyberattack began, Clark Hill turned to Duff & Phelps instead of, rather than separate from or in addition to, eSentire, to do the necessary investigative work. The firm has pointed to no documents reflecting eSentire’s
doing investigative or remedial work after September 14, even though, from all indications, the attack was potentially still ongoing and the firm did not yet have a full understanding of its cause or scope. See ECF No. 38-1 at ECF p. 1 (September 13 email from eSentire providing “not necessarily complete” timeline of attack and noting that network “may be compromised”); ECF No. 38 (eSentire-produced “Event Timeline” showing potential suspicious activity continuing on September 14); ECF No. 25-3 at 1 (letter from Clark Hill's General Counsel dated September 19 stating that firm's “investigation regarding the nature and extent of the cyberattack [was] continuing”). And at precisely the time the “trail essentially goes cold” as to eSentire's work, see ECF No. 33 (Reply) at 10, Duff & Phelps's began: Rousseau reported that at 1:30 p.m. on the 14th, he “[s]poke with Duff and Phelps to request help with incident” and that the “Duff and Phelps team arrive[d] on-site and beg[an] investigation” at 11:45 p.m. that evening. See ECF No. 38 at ECF p. 3. Internal emails also show that Rousseau and Clark Hill's General Counsel, Edward Hood, held a call the morning of the 15th with Duff & Phelps employees, referring to them as “the incident response team.” ECF No. 41-1 at ECF p. 2. The Report confirms this timeline of Duff & Phelps's involvement.

There is more. Hood himself admits that the Report was shared not just with outside and in-house counsel, but also with “select members of Clark Hill's leadership and IT team.” Opp. at 6 (citing ECF No. 29-27 (Declaration of Edward J. Hood), ¶¶ 5–6). Hood further avers that the Report was used to “assist[ ] [Clark Hill] in connection with managing any issues, including”—but notably not limited to—“potential litigation ... related to the ... cyber incident.” Hood Decl., ¶ 6 (emphasis added). Defendant also shared the report with the FBI “as part of the FBI's investigation of the cyber incident.” Id. The Report was probably shared this widely, as Plaintiffs would not have been produced in the absence of litigation, and that, on the same day, MPG in turn retained Duff & Phelps, Duff & Phelps's role seems to have been far broader than merely assisting outside counsel in preparation for litigation. Although Clark Hill papered the arrangement using its attorneys, that approach “appears to [have been] designed to help shield material from disclosure” and is not sufficient in itself to provide work-product protection. See also Dominion Dental, 429 F. Supp. 3d at 194 (finding defendant's “conclusory statement” in affidavit that report was prepared in anticipation of litigation “rebutted by extensive evidence in the record”); Premera II, 329 F.R.D. 656, 666 (D. Or. 2019) (concluding that defendant “cannot shield [consultant forensic work] from discovery by delegating [its] supervision to counsel”); see also Allied Irish Banks v. Bank of Am., N.A., 240 F.R.D. 96, 99 (S.D.N.Y. 2007) (“That [the plaintiff] hired a law firm to 'assist' in the investigation is of no moment.... A party may not insulate itself from discovery by hiring an attorney to conduct an investigation that otherwise would not be accorded work product protection.”) (cleaned up).

At a minimum, it is Clark Hill's burden to demonstrate that a substantially similar document to the Duff & Phelps Report would not have been produced in the absence of litigation, and it has fallen well short of doing so. Both the Report and related materials (referred to by Defendant as “Expert Materials,” Opp. at 11) are accordingly not protected work product.

2. Attorney-Client Privilege
[6] [7] Distinct from the work-product privilege, the attorney-client privilege protects “a confidential communication between attorney and client if that communication was made for the purpose of obtaining or providing legal advice to the client.” In re Kellogg Brown & Root, Inc., 756 F.3d 754, 757 (D.C. Cir. 2014). The Duff & Phelps Report does not exactly fit within that canonical formulation, as it is not a communication between an attorney and a client, but rather one between an attorney and an outside consultant hired by the attorney. See In re Sealed Case, 676 F.2d 793, 809 (D.C. Cir. 1982) (stating that generally, “communications that do not involve both attorney and client ... are unprotected”). Although Defendant is not explicit, its unstated argument seems clear enough: the privilege also “can attach to reports of third parties made at the request of the attorney or the client where the purpose of the report was to put in usable form information obtained from the client.” TRW, 628 F.2d at 212 (citing United States v. Kovel, 296 F.2d 918 (2d Cir. 1961)). The classic example is a report by an accountant who, like a translator, takes the client's tax or financial information and makes it digestible to the attorney. Id. Clark Hill's argument, then, is that the Duff & Phelps Report qualifies as privileged per this doctrine.

[8] [9] It does not. As the Circuit has explained, the Kovel doctrine must be applied narrowly “lest the privilege be construed to engulf ‘all manner of services’ that should not be summarily excluded from the adversary process.” Linde Thomson Langworthy Kohn & Van Dyke, P.C. v. Resolution Tr. Corp., 5 F.3d 1508, 1514–15 (D.C. Cir. 1993) (quoting TRW, 628 F.2d at 212); see also In re Lindsey, 158 F.3d 1263, 1272 (D.C. Cir. 1998) (“The attorney-client privilege must be strictly confined within the narrowest possible limits consistent with the logic of its principle.”) (cleaned up). After all, unlike the work-product privilege, which may be overcome by a sufficient showing of need, the attorney-client privilege is absolute. To that end, the Kovel court itself made clear that, for instance, “if the advice sought [by the client] is the accountant's rather than the lawyer's, no privilege exists” over the accountant's report. Kovel, 296 F.2d at 922; see also TRW, 628 F.2d at 212 (same).

[10] From the factual record discussed above and the Report itself, the Court concludes that Clark Hill's true objective was gleaning Duff & Phelps's expertise in cybersecurity, not in “obtaining legal advice from [its] lawyer.” Linde Thomson, 5 F.3d at 1514 (quoting TRW, 628 F.2d at 212). At a minimum, Defendant has not demonstrated that the opposite is true. Duff & Phelps undertook a full investigation — the only one apparently commissioned by Clark Hill — with the goal of determining how the attack happened and what information was exfiltrated. The Report provides not only a summary of the firm's findings, but also pages of specific recommendations on how Clark Hill should tighten its cybersecurity. And it was shared with both Clark Hill IT staff and the FBI, presumably with an eye toward facilitating both entities' further efforts at investigation and remediation. (Because the Court finds the Report not subject to attorney-client privilege, it does not address Plaintiff's separate argument that Defendant waived the privilege by disclosing the Report to the FBI. See Reply at 17–21.)

The firm points to only one case, the Target decision, that has applied the attorney-client privilege to a similar forensic report, and that non-binding decision (even assuming it is correct) is distinguishable in at least three ways. First, as discussed above, Target had a two-track approach, with one track a concededly “non-privileged investigation .... set up so that Target ... could learn how the breach happened and ... respond to it appropriately.” 2015 WL 6777384, at *2. Assuming that investigation was sufficient for Target's business purposes, it is much easier to view the other as aimed at facilitating effective legal representation. Second, and relatedly, there is no indication that the Target report was shared as widely for non-legal purposes as the Duff & Phelps Report. Third, the Target court specifically noted that the relevant investigation and report were not “focused ... on remediation of the breach.” Id. at *3. Here, Duff & Phelps was apparently engaged for immediate “incident response” and began its work as the attack was thought to still be ongoing. Its Report, moreover, includes pages of specific remediation advice.

For the foregoing reasons, the Duff & Phelps Report and associated materials are not privileged and must be disclosed, and the related interrogatories must be answered.

B. Other Clark Hill Clients

Defendant separately resists Plaintiff's discovery requests for information relating to the effect of the cyberattack on firm
clients other than Guo himself. See Opp. at 22–24. For instance, Plaintiff has served a request for production seeking “[a]ll documents reflecting that the ‘hacking’ ... resulted in a third party's obtaining ... information, data, or material regarding any Clark Hill client other than or in addition to plaintiff.” ECF No. 29-18 (March 11 RFP), ¶ 18. Clark Hill claims that this sort of information is both irrelevant and privileged. See Opp. at 22–23. Here, too, the Court will grant Plaintiff's Motion to Compel: the information is clearly relevant, and appropriate redactions can assuage any privilege or privacy concerns.

[11] As to relevance, the scope of the attack is directly germane to a central issue in the case — namely, in Defendant's own words, “the sufficiency and reasonableness of Clark Hill's cybersecurity in September 2017.” Id. at 23. One easily conjured example: if the attack was largely focused on Plaintiff, that might suggest that a reasonable custodian of his documents should have been aware that he in particular was a target and should thus have taken appropriate special precautions. If the attack, conversely, was more of a fishing expedition aimed at a wide swath of the firm's closely held information, that might suggest the opposite. Or perhaps, if the attack was indeed broad, one could argue that a reasonably prudent custodian should have detected it sooner. In short, the sort of information Plaintiff seeks is directly relevant; and even if it were not, there is a "reasonable likelihood that allowing discovery of the[se] documents will lead to discovery of [other] evidence [that is] relevant," which renders them discoverable under Rule 26. Food Lion, Inc. v. United Food & Commercial Workers Intl' Union, AFL-CIO-CLC, 103 F.3d 1007, 1013 (D.C. Cir. 1997).

[12] [13] The firm also contends that it cannot fully answer interrogatories or turn over documents relating to the hack's effect on its other clients because doing so would reveal that it represents those individuals, and the fact of representation itself is attorney-client privileged. See Opp. at 3, 24. That does not quite state the law accurately. As this Court has previously explained, “Under the general rule, the attorney-client privilege does not protect from disclosure the identity *15 of the client ... and the general purpose of the work performed.” Cause of Action Inst. v. U.S. Dep't of Justice, 330 F. Supp. 3d 336, 350 (D.D.C. 2018) (citation and internal quotation marks omitted). On the other hand, “when a client's identity is sufficiently intertwined with the client's confidences,” the privilege does apply. Id. (cleaned up and citations omitted). At this point, Defendant (which bears the burden to demonstrate that the privilege applies) has given the Court no way of knowing whether the latter situation is applicable to any documents at issue.

That said, however, privilege is not the only consideration here. Discovery must be both “relevant” and “proportional to the needs of the case,” Fed. R. Civ. P. 26(b)(1), and the Court doubts that the precise identity of any Clark Hill client is relevant to the issues here. To the extent that it is, its germaneness is likely weak enough to be outweighed by the clients' privacy interests. See Henson v. Turn, Inc., No. 15-1497, 2018 WL 5281629, at *5 (N.D. Cal. Oct. 22, 2018) (“Courts and commentators have recognized that privacy interests can be a consideration in evaluating proportionality ....”). It thus seems to the Court that Defendant can fully safeguard the identity of its clients and any of their confidences, if applicable, with appropriate redactions in responsive documents and with tailored interrogatory answers. There is no basis, however, for its blanket refusal to respond to Plaintiff's requests for production, and the Court will grant the Motion to Compel that discovery subject to appropriate redactions.

III. Conclusion

For the foregoing reasons, the Court will grant Plaintiff's Motion to Compel. A contemporaneous Order so stating will issue this day.

All Citations

338 F.R.D. 7
MEMORANDUM OPINION AND ORDER

John F. Anderson, United States Magistrate Judge

This matter is before the court on plaintiffs' motion to compel production of Mandiant Report and related materials. (Docket no. 412). Plaintiffs have filed a memorandum in support (Docket nos. 413, 416), Capital One has filed an opposition (Docket no. 435), and plaintiffs have filed a reply (Docket nos. 445, 447). The court heard argument on this motion on May 15, 2020. Having reviewed the pleadings filed by the parties and considered the arguments raised by counsel, and for the reasons stated below, the court finds that Capital One has not carried its burden of establishing that the Mandiant Report is entitled to protection under the work product doctrine.

Background
Capital One entered into a Master Services Agreement (“MSA”) with FireEye, Inc., d/b/a Mandiant (“Mandiant”) on November 30, 2015, and thereafter entered into periodic Statements of Work (“SOW”) and purchase orders with Mandiant pursuant to the MSA. (Blevins Decl. ¶ 4, Docket no. 435-1). As stated by Jeffrey Blevins II, a senior manager of Capital One's Cyber Security Operations Center, “one purpose of the MSA and associated SOWs was to ensure that Capital One could quickly respond to a cybersecurity incident should one occur. As a financial institution that stores financial and other sensitive information, it is critical that Capital One be positioned to immediately respond to any potential compromise of the security of its systems.” (Id. at ¶ 5). The SOWs with Mandiant provided for incident response services in the event such services were necessary. (Id. at ¶ 6). Capital One paid Mandiant a retainer for the SOW that was executed with Mandiant on January 7, 2019, and it entitled Capital One to 285 hours of services from Mandiant. (Id. at ¶ 8). In February 2019 Capital One designated the retainer paid to Mandiant as a “Business Critical” expense and not a “Legal” expense. (Docket no. 416-3 at 13, Docket no. 435 at 18). The SOW between Capital One and Mandiant in 2019 provided that Mandiant would provide incident response services during the covered period in the following areas: computer security incident response support; digital forensics, log, and malware analysis support; and incident remediation assistance and that Mandiant would provide a detailed final report covering the engagement activities, results and recommendations for remediation in a written detailed technical document. (Docket no. 416-2 at 3–4).

As described in detail in the Corrected Representative Consumer Class Action Complaint (Docket no. 354), in March 2019 a data breach occurred whereby an unauthorized person gained access to certain types of personal information relating to Capital One customers. In its opposition, Capital One states that on July 19, 2019, it confirmed that a data breach had occurred. (Docket no. 435 at 6). On July 20, 2019, Capital One retained Debevoise & Plimpton (“Debevoise”) to provide legal advice in connection with the data breach incident. (Cantwell Decl. ¶ 3, Docket no. 435-2). On July 24, 2019, Debevoise and Capital One signed a Letter Agreement with Mandiant whereby Mandiant agreed to provide services and advice concerning “computer security incident response; digital forensics, log, and malware analysis; and incident remediation.” (Docket no. 435-2 at 6–8). The Letter Agreement provides that the payment terms were to be the same as those set out in the SOW dated January 7, 2019, between Capital One and Mandiant and the parties would abide by the applicable terms in the SOW and MSA between Capital One and Mandiant dated November 30, 2015. (Id.). While the Letter Agreement provides for the same services to be performed by Mandiant under the same terms as the SOW and MSA, the Letter Agreement provides that the work would be done at the direction of counsel and the deliverables would be provided to counsel instead of Capital One. (Id.). On July 26, 2019, an addendum to the Letter Agreement was prepared whereby the engagement of services would also include penetration testing of systems and endpoints. (Id. at 10).

*2 On July 29, 2019, Capital One issued a public announcement concerning the data breach. (Cantwell Decl. ¶ 3). The following day the first of many lawsuits was filed against Capital One asserting claims based on the data breach. See Baird v. Capital One Fin. Servs. Corp.,
Mandiant preformed the services that had been outlined in the Letter Agreement and prepared a report “detailing the technical factors that allowed the criminal hacker to penetrate Capital One's security.” (Cantwell Decl. ¶ 19). The Mandiant Report was issued on September 4, 2019. (Docket no. 435 at 10). Mandiant was paid for its initial work under the Letter Agreement out of the retainer already provided to Mandiant under the January 7, 2019 SOW between Mandiant and Capital One. (Watts Decl. ¶ 3, Docket no. 435-3). After the retainer amount was exhausted, Mandiant's additional fees were paid directly by Capital One through the budget for the Cyber organization. (Id. ¶ 4). In December 2019 the expenses associated with the work Mandiant performed relating to the data breach were re-designated as legal expenses and deducted against Capital One's legal department's budget. (Id. at ¶ 5).

In addition to Mandiant, an internal investigation into the data breach was instituted involving a manager from Capital One's cyber incident management team and the Chief Information Security Officer that was separate from, and proceeded parallel to, Mandiant's investigation. (Blevins Decl. ¶ 16). Capital One has identified certain internal and external investigations that were undertaken in response to the data breach incident in its answer to plaintiffs’ interrogatory number 11 (Docket no. 416-13 at 22–23) indicating that it does not “categorically claim work product protection or privilege over all of these company-led investigations” and “will produce documents relating to certain of them” (Docket no. 435 at 16). The brief summary of the work conducted and description of the results of the internal investigations set forth in the response to interrogatory number 11 is not sufficient for the court to determine the full nature and extent of those investigations and how the results were used within Capital One. Furthermore, Capital One has provided no detail concerning which of these internal investigations it will be producing documents for and the extent of its document production concerning those internal investigations.

The Mandiant Report was initially sent to Debovoise, which in turn provided the report to “Capital One's legal department.” (Cantwell Decl. ¶ 20). Debovoise also provided the Mandiant Report to Capital One's Board of Directors. (Id. at ¶ 22). Exhibit 2 to Capital One's opposition states that it contains “a list of those to whom the Mandiant report was disclosed.” (Docket no. 435-5). This list includes approximately fifty Capital One employees, four regulators (Federal Deposit Insurance Corporation, Federal Reserve Board, Consumer Financial Protection Bureau, and Office of the Comptroller of the Currency), and an accounting firm (Ernest & Young). (Id.). There is no explanation provided as to why each recipient was provided with a copy of the Mandiant Report and whether the disclosure was related to a business purpose or for the purposes of litigation. Even for those within the legal department, it is unclear if they were provided with the Mandiant Report in relation to duties involving the litigation or for regulatory or other business reasons. While the Cantwell declaration states the Mandiant Report was distributed to Capital One's Board of Directors, the list provided by Capital One's counsel does not appear to include those individuals. While there is an item named “corporate governance office general email box” on the list, there is no indication who has access to that “general email box.” Capital One's opposition also fails to address what, if any, restrictions were placed on those persons and entities who received a copy of the Mandiant Report on discussing, copying, or providing the Mandiant Report, or any portion of it, to others.

As described in the Cantwell declaration, during Mandiant's investigation, it had communications with Ernst & Young, Capital One's outside auditor, related to Mandiant's confirmation of certain facts so that Ernst & Young was able to conclude that the data breach had no impact on Capital One's internal controls over financial accounting. (Cantwell Decl. ¶¶ 13, 14, see also Docket no. 416-6). It also appears that individuals within Capital One anticipated using the Mandiant Report in making certain disclosures required under the Sarbanes Oxley Act (Docket no. 416-4) and that the Mandiant Report was provided to an employee “for 2nd line business need” (Docket no. 416-11).

Legal Standards
In large part the parties agree on the legal principles involved. First, there is no dispute that Capital One, the party asserting work product doctrine, bears the burden of demonstrating the applicability of that doctrine. Solis v. Food Employers Labor Relations Ass'n, 644 F.3d 221, 232 (4th Cir. 2011), Sandberg v. Virginia Bankshares, Inc., 979 F.2d 332, 355 (4th Cir. 1992). Also, it is well-established that courts generally disfavor assertions of evidentiary privileges because they shield evidence from the truth-seeking process; as such, they are to be narrowly and strictly construed so that they are confined to the narrowest possible limits consistent with the logic of its principle. In re Grand Jury
the work product doctrine bears the burden of showing how


Federal Rule of Evidence 502 defines work-product protection as “the protection that applicable law provides for tangible material (or its intangible equivalent) prepared in anticipation of litigation or for trial.” Fed. R. Evid. 502(g)(2).

As the Fourth Circuit discussed in National Union Fire Ins. Co. v. Murray Sheet Metal Co., 967 F.2d 980, 984 (4th Cir. 1992), the fact that there is litigation does not, by itself, cloak materials with work product immunity but the material must be prepared because of the prospect of litigation. Materials prepared in the ordinary course of business or pursuant to regulatory requirements or for other non-litigation purposes are not documents prepared in anticipation of litigation. Id.

In order to be entitled to protection, a document must be prepared “because of” the prospect of litigation and the court must determine “the driving force behind the preparation of each requested document” in resolving a work product immunity question. Id.

In RLI, Judge Payne thoroughly discussed the National Union decision and interpreted the “because of” standard in that decision. RLI, 477 F. Supp. 2d at 746-49. The “because of standard” is designed to protect only work that was conducted because of the litigation and not work that would have been done in any event. Id. at 747. The work product doctrine withholds protection from documents that would have been created in essentially similar form irrespective of the litigation. Id. Accordingly, work product protection applies when the party faces an actual claim or a potential claim following an actual event or series of events that reasonably could result in litigation and the work product would not have been prepared in substantially similar form but for the prospect of that litigation. 2 Id. at 748.

Analysis

*4 There is no question that at the time Mandiant began its “incident response services” in July 2019, there was a very real potential that Capital One would be facing substantial claims following its announcement of the data breach. Therefore, the determinative issue is whether the Mandiant Report would have been prepared in substantially similar form but for the prospect of that litigation.

As recognized in RLI, the party requesting protection under the work product doctrine bears the burden of showing how it would have investigated the incident differently if there was no potential for litigation. RLI, 477 F. Supp. 2d at 749-50. The hiring of outside counsel does not excuse a company from conducting its duties and addressing the issues at hand. Id. As in RLI, the fact that the investigation was done at the direction of outside counsel and the results were initially provided to outside counsel, does not satisfy the “but for” formulation. For the reasons discussed below, Capital One has not presented sufficient evidence to show that the incident response services performed by Mandiant would not have been done in substantially similar form even if there was no prospect of litigation.

Capital One had a long-standing relationship with Mandiant and had a pre-existing SOW with Mandiant to perform essentially the same services that were performed in preparing the subject report. The services to be provided in the January 7, 2019 SOW are the same services described in the Letter Agreement. Capital One's senior manager of the cyber security operations center and the person responsible for managing Capital One's relationship with Mandiant acknowledged that as a financial institution that stores sensitive financial and other sensitive information, it is critical that it be positioned to immediately respond to any potential compromise of the security of its systems. (Blevins Decl. ¶ 5). The retainer paid to Mandiant was considered a business-critical expense and not a legal expense at the time it was paid. While the fact that the Mandiant Report was provided to four different regulators and to Capital One's accountant may not necessarily constitute a waiver, it does show that the results of an independent investigation into the cause and the extent of the data breach was significant for regulatory and business reasons. This independent investigation was also used internally for Sarbanes Oxley disclosures and was referenced in a draft FAQs prepared by a senior vice president for finance prior to the public announcement of the data breach. (Docket no. 436-12). 3 The only significant evidence that Capital One has presented concerning the work Mandiant performed is that the work was at the direction of outside counsel and that the final report was initially delivered to outside counsel. Capital One's outside counsel states that Mandiant issued a written report detailing the technical factors that allowed the criminal hacker to penetrate Capital One's security. There is no statement by Capital One, or evidence upon which one could find, that Capital One would not have called upon Mandiant to perform the services described in the SOW that existed prior to the data breach and prepare a written report as provided in the SOW that would have detailed the results of its investigation, including
detailing the technical factors that allowed the criminal hacker to penetrate Capital One's security.


In Experian, the court applied the same test as applied by Judge Payne in RLI and followed in this decision – that is, considering the totality of the circumstances can it fairly be said that the document was created because of anticipated litigation and would not have been created in substantially similar form but for the prospect of that litigation. Experian, 2017 WL 4325583 at *1. In finding that the report was protected as work product, the court noted that Experian immediately retained outside counsel and that outside counsel hired Mandiant to prepare a report. The court emphasized the timing of the retention of Mandiant by outside counsel and the fact the full report was not given to Experian's incident response team. The court stated that if the report “was more relevant to Experian's internal investigation or remediation effort, as opposed to being relevant to defense of the litigation, then the full report would have been given to that team.” Id. at *3. The court then concluded that the report would not have been prepared in substantially the same form or with the same content. Id. One significant difference between the facts in Experian and the facts in this case is that Capital One had an existing SOW and MSA with Mandiant at the time of the data breach that was effectively transferred to outside counsel. As set out in the SOW and Letter Agreement, the work to be performed by Mandiant was the same, the terms were the same, but the work was to be performed at the direction of outside counsel and the final report delivered to outside counsel. The retention of outside counsel does not, by itself, turn a document into work product. While it is true that in Experian the report was not given to Experian's response team, it appears that at least several members of Capital One's cyber technical, enterprise services, information security and cyber teams were provided with a copy of the Mandiant Report, and that it was used by Capital

One for various business and regulatory purposes. As each case must be determined on its own facts and circumstances, the court cannot come to the same conclusion as the court in Experian that the work performed by Mandiant would not have been done in substantially the same form or with the same content.

The order in Arby's does not address in detail the facts underlying the ruling or the legal analysis for the conclusion that Arby's hired Mandiant to produce a report in anticipation of litigation and for other legal reasons and it is protected as work product and a privileged attorney-client communication. Arby's, No. 1:17mi55555-WMR (Docket no. 445-3). Accordingly, the court can divine no guidance from this decision.

In Target, the court also issued a brief order announcing its decision in which it provided very little factual background and no legal analysis on the work product issue. Target, 2015 WL 6777384. In essence this order merely announces a ruling on several challenged documents following an in camera review by the court and provides no assistance in resolving this case.

*6 As in Arby's and Target, the order entered in Genesco referring to reasons stated in open court for its rulings provides no substantive guidance on the issues involved in this case. Genesco, No. 3:13-cv-00202 (Docket no. 445-2).

Plaintiffs have provided the court with two data breach cases that the court finds persuasive, one from the District of Oregon and one from this court. The decision in Premera, contains a discussion of the work product doctrine and how one should consider the application of that doctrine when materials are prepared for “dual purposes.” In re Premera Blue Cross Customer Data Sec. Litig., 296 F. Supp. 3d 1230 (D. Or. 2017). The Premera court indicated that courts must view the totality of the circumstances and determine whether the document would have been created in substantially similar form but for the prospect of litigation. In discussing the Mandiant Remediation Report, the court noted that Mandiant was performing work for Premera and discovered the existence of malware in Premera's system. Premera then hired outside counsel and entered into an amended statement of work that shifted supervision of Mandiant's work to outside counsel. The amended statement of work did not otherwise change the scope of Mandiant's work from what was described in the master services agreement.
The court distinguished the decision in Target on the basis that there was an independent data breach investigation performed by the company “that was produced in discovery” and that the attorneys performed a separate investigation through a retained expert company. The decision in Experian was distinguished because outside counsel hired Mandiant and in Premera, Mandiant had already been hired and was performing services for Premera before outside counsel became involved. The court also recognized that Premera had the burden of showing Mandiant changed the nature of its investigation at the instruction of outside counsel and that Mandiant's scope of work and purpose became different when outside counsel became involved.

Capital One attempts to distinguish this decision on the basis that at the time of the data breach Mandiant was not performing an ongoing investigation. While it is true that there was no ongoing investigation at the time of the data breach or its subsequent discovery, the court finds the fact that there was an existing SOW with a paid retainer that obligated Mandiant to perform 285 hours of service for Capital One in 2019, at the time of the data breach and its discovery, to be significant. Again, Capital One has not carried its burden of showing that Mandiant's scope of work under the Letter Agreement with outside counsel was any different than the scope of work for incident response services set forth in the existing SOW and that it would not have been performed without the prospect of litigation.

Finally, the court also finds the Dominion Dental decision from this court to be particularly helpful. In re Dominion Dental Servs. USA, Inc. Data Breach Litig., 2019 WL 7592343 (E.D. Va. Dec. 19, 2019). In that decision the court found that the defendants had failed to show that the Mandiant report would not have been completed in substantially similar form but for the prospect of litigation and granted the motion to compel. Id. at *5. In Dominion Dental the defendants argued that the Mandiant report “was created to inform legal counsel and litigation strategy” and was therefore protected work product. Id. at *1. Dominion Dental had hired Mandiant prior to the data breach involved in that case to investigate, prevent, and remediate data breaches. Id. At the time of the data breach, Dominion Dental and its outside counsel had a statement of work with Mandiant whereby Mandiant was to provide incident response services including “computer incident response support, digital forensics support, advanced threat actor support, and advanced threat/incident assistance.” Id. After the data breach was discovered, Dominion Dental's outside counsel then entered into another statement of work with Mandiant incorporating the previous statement of work and master services agreement and including virtually the same deliverables as the statement of work that was in existence prior to the data breach. Id. at *2. Dominion Dental noted a reference in a list of talking points to retaining Mandiant, a world leading cyber security firm, to investigate the incident and that the Mandiant report appears to have been used with Dominion Dental's regulators. Id. The court discussed the same decisions cited by the parties in this case, Experian and Target relied upon by Capital One and Premera relied upon by the plaintiffs. Id. at *3. Even in the face of a statement in an affidavit from Dominion Dental that the Mandiant report would not have been prepared in a substantially similar form and may not have been necessary at all without the threat of litigation, the court found Dominion Dental had not carried its burden, relying heavily upon the fact that the description of services in the statement of work in existence prior to the data breach was “almost identical” to the services in the post-data breach statement of work. Id. at *4. The fact that the post-data breach statement of work indicated that the work was to be “under the direction of Counsel” did not alter the business purposes of the work to be performed and appeared to be designed to help shield the report from disclosure. Id.

*7 Capital One's attempts to distinguish the Dominion Dental decision are unpersuasive. First, Capital One has not shown that the nature of the work Mandiant had agreed to perform changed when outside counsel was retained. As discussed in detail above, and as was the case in Dominion Dental, the statement of works and master services agreements provided for virtually identical services to be performed before and after the data breaches were discovered. The fact that Dominion Dental waited two months to make a public announcement after it learned of the intrusion, at which time Mandiant had concluded its report, does not alter the legal analysis. Just as Capital One has argued here, that there “is no question that the Cyber Incident was the type of event that Capital One knew would lead to litigation” (Docket no. 435 at 12), there can be no question that Dominion Dental knew there was a prospect of litigation once the data breach had been discovered. Finally, Capital One argues that “there was no evidence” in Dominion Dental that the fruits of Mandiant's work were used for legal purposes. However, the record in Dominion Dental included an affidavit that the Mandiant report would not have been prepared in substantially similar form without the threat of litigation and
that the statement of work was modified to provide that the work was to be performed under the direction of counsel and if requested by counsel.

For these reasons, it is hereby

ORDERED that plaintiffs' motion to compel is granted in part. Capital One shall provide plaintiffs with a copy of the Mandiant Report pursuant to the terms of the Protective Order entered in this action. In accordance with Local Civil Rule 37(C), Capital One shall have eleven days to comply with this order. The plaintiffs' motion to compel “related materials” is denied without prejudice. As discussed in Capital One's opposition, the issues concerning all related materials is not ripe for decision. (Docket no. 435 at 28–30). The parties have not had an opportunity to discuss the claim of privilege over related materials and to consider any arguments that certain related materials may be entitled to be withheld from production even if the Mandiant Report was found not to be entitled to work product protection.

All Citations
Slip Copy, 2020 WL 2731238

Footnotes

1 The description of services in the Letter Agreement are the same as those set forth in the SOW dated January 7, 2019, between Capital One and Mandiant. (Docket no. 416-2 at 3).

2 Given the ruling on the work product issue based on the “because of” standard, it is not necessary to address the waiver or substantial need issues discussed by the parties in their briefs. That said, it appears that the waiver argument may have some merit given the lack of evidence presented in this motion concerning the distribution of the Mandiant Report and what protections were taken to avoid having the Mandiant Report or the information contained therein disclosed to a person or entity in an adversarial relationship. As to substantial need, while it would be more efficient for the plaintiffs to have the results of Mandiant's investigation, based on current record it appears that the event logs and network diagrams reviewed by Mandiant may be available to the plaintiffs.

3 Capital One refers to these as “investor relations ‘talking points’” in its opposition and argues that plaintiffs have offered no evidence showing these talking points were ever used. (Docket no. 435 at 18). However, Capital One has not provided any evidence that the talking points were not used.
2021 WL 3733137
Only the Westlaw citation is currently available.
United States District Court, M.D. Pennsylvania.

IN RE RUTTER'S DATA SECURITY BREACH LITIGATION

CIVIL ACTION NO. 1:20-CV-382
| Signed 07/22/2021

ORDER

KAROLINE MEHALCHICK, United States Magistrate Judge

*1 Now before the Court is a discovery dispute regarding the production of an investigative report which was created after Defendant was notified of a potential data breach. (Plaintiffs' Letter, June 15, 2021; Defendant's Letter, June 15, 2021). Plaintiffs request an order compelling the production of “an investigative report created in response to the data breach by a third-party cybersecurity consultant—Kroll Cyber Security, LLC (“Kroll”)—and any related communications between Kroll and Defendant …” (Plaintiffs' Letter, June 15, 2021) (“Plfs' 6/15 Letter”). Defendant asserts that this material is protected by both the work product doctrine and the attorney-client privilege. (Defendant's Letter, June 15, 2021) (“Def's 6/15 Letter”). Defendant asserts that this material is protected by both the work product doctrine and the attorney-client privilege. (Defendant's Letter, June 15, 2021) (“Def's 6/15 Letter”).


A. THE WORK PRODUCT DOCTRINE

Defendant asserts that the report prepared by Kroll after Defendant was alerted of possible fraudulent activity (the “Kroll Report”) is protected from discovery by the work product doctrine. (Def's 6/15 Letter). The work product doctrine serves to “promote[ ] the adversary system directly by protecting the confidentiality of papers prepared by or on behalf of attorneys in anticipation of litigation. Protecting attorneys' work product promotes the adversary system by enabling attorneys to prepare cases without fear that their work product will be used against their clients.” Westinghouse Elec. Corp. v. Republic of Philippines, 951 F.2d 1414, 1428 (3d Cir. 1991). The work product doctrine directly promotes the adversary system, whereas the attorney-client privilege serves to directly promote the attorney-client relationship. Westinghouse Elec. Corp, 951 F.2d at 1428. The Supreme Court of the United States has said that the work product doctrine “shelters the mental processes of the attorney, providing a privileged area within which he can analyze and prepare his client's case.” United States v. Nobles, 422 U.S. 225, 238 & n. 11 (1975).

*2 The doctrine applies to “documents and tangible things ... prepared in anticipation of litigation or for trial by or for another party or by or for that other party's representative (including the other party's attorney, consultant, surety, indemnitor, insurer, or agent) ...” In re Cendent Corp. Securities Litigation, 343 F.3d 658, 662 (3d Cir. 2003) (quoting Fed. R. Civ. P. 26(b)(3)). Rule 26(b)(3) establishes two types of work product: first, general documents and tangible things that are prepared in anticipation of litigation, and second, work product that consists of “mental impressions, conclusions, opinion, or legal theories of an attorney or other representative of a party concerning the litigation.” Cendent Corp, 343 F.3d at 663 (quoting Fed. R. Civ. P. 26(b)(3)). The party seeking the protection of the work
product doctrine has the burden of proving that the doctrine applies. Conoco, Inc. v. U.S. Dep't of Justice, 687 F.2d 724, 730 (3d Cir. 1982).

For the work product doctrine to apply, the document must be prepared “in anticipation of litigation.” Fed. R. Civ. P. 26(b) (3). A document is prepared in anticipation of litigation if “in light of the nature of the document and the factual situation of the particular case, the document can fairly be said to have been prepared or obtained because of the prospect of litigation.” Martin v. Bally's Park Place Hotel & Casino, 983 F.2d 1252, 1258 (3d Cir. 1993) (quoting United States v. Rockwell Intern., 897 F.2d 1255, 1266 (3d Cir. 1990)). Aiding in “identifiable” or “impending” litigation must have been the “primary motivating purpose behind the creation of the document.” United States v. Rockwell Intern., 897 F.2d 1255, 1266 (3d Cir. 1990); Leonen v. Johns-Manville, 135 F.R.D. 94, 97 (D.N.J. 1990). To determine whether “the prospect of litigation” is the purpose behind the document, the initial inquiry is into whether the party which ordered or prepared the document had a “unilateral belief” that litigation would result. Martin, 983 F.2d at 1260. Second, the anticipation of litigation must be objectively reasonable. Martin, 983 F.2d at 1260, 1

It is clear from the contract between Kroll and Defendant that the primary motivating purpose behind the Kroll Report was not to prepare for the prospect of litigation. Included in the contract is a “statement of work” (SOW) which includes a description of services. (Def's 6/15 Letter, at 14). The following is included in the “Description of Services” section of the SOW: “The overall purpose of this investigation will be to determine whether unauthorized activity within the Rutter's systems environment resulted in the compromise of sensitive data, and to determine the scope of such a compromise if it occurred.” (Def's 6/15 Letter, at 14). This language demonstrates that Defendant did not have a unilateral belief that litigation would result at the time it requested the Kroll Report. See Martin, 983 F.2d at 1260. The purpose of the investigation was to determine whether data was compromised, and the scope of such compromise if it occurred. (Def's 6/15 Letter, at 14). Without knowing whether or not a data breach had occurred, Defendant cannot be said to have unilaterally believed that litigation would result. (Def's 6/15 Letter, at 14); see Martin, 983 F.2d at 1260.

Furthermore, in its corporate deposition, Defendant stated that litigation was not contemplated at the time the Kroll Report was prepared. (Plfs' 6/15 Letter, at 17). Rutter's corporate designee, Bernard Frazer, is the individual who signed the agreement with Kroll to perform the investigation at issue and write the Kroll Report. (Def's 6/15 Letter, at 9-16; Plfs' 6/15 Letter, at 1). Frazer testified that he was not “contemplating” forthcoming lawsuits as a result of the data breach at the time Kroll was performing its work and that he was unaware of anyone else at Rutter's contemplating such lawsuits. (Plfs' 6/15 Letter, at 17). According to Defendant, “Kroll would have prepared – done this work and prepared its incident response investigation regardless of whether or not lawsuits were filed six months later.” (Plfs' 6/15 Letter, at 17-18). As such, it cannot be said that the “primary motivating factor” behind the creation of the Kroll Report was to aid in identifiable or impending litigation. See Rockwell Intern., 897 F.2d at 1266 (holding that for the work product doctrine to apply, litigation must have been the “primary motivating purpose behind the creation of the document”); Leonen, 135 F.R.D. at 97 (D.N.J. 1990) (holding that there must have been an identifiable specific claim or impending litigation when the materials were prepared).

*3 Defendant cites In re Experian Data Breach Litig., No. SACV1501592AGDFMX, 2017 WL 4325583, at *2 (C.D. Cal. May 18, 2017) in support of its position that the Kroll Report was prepared in anticipation of litigation. (Def's 6/15 Letter, at 3-4). In Experian, the investigative report was provided to Experian's outside litigation counsel, which then provided it to Experian's in-house counsel, and was not provided to Experian's Incident Response Team. Experian, 2017 WL 4325583, at *2. Here, Kroll provided its report to Defendant when it was completed and there is no evidence that it was provided first to BakerHostetler. (Plfs' 6/15 Letter, at 14, 16) (Defendant testifying that Kroll's work concluded towards end of July 2019 and that the Kroll Report was delivered to Defendant around July of 2019). Kroll was to “work alongside Rutter's IT personnel to identify and remediate any potential vulnerabilities.” (Def's 6/15 Letter, at 14) (emphasis added). In Experian, the report's legal nature was supported by declarations. Experian, 2017 WL 4325583, at *2. Unlike the declarations in Experian, Rutter's corporate designee testified that he was unaware of anyone at Rutter's contemplating a lawsuit at the time the Kroll Report was compiled. (Plfs' 6/15 Letter, at 17). 2 Similarly, the report in In re Target Corp. Customer Data Sec. Breach Litig., 2
MDL No. 14-2522, 2015 WL 6777384 (D. Minn. Oct. 23, 2015) was compiled after litigation was already pending and more was reasonably expected to follow. Target, 2015 WL 6777384, at *3.

For the foregoing reasons, production of the Kroll Report and related communication between Kroll and Defendant are not precluded by the work-product doctrine.

B. THE ATTORNEY-CLIENT PRIVILEGE

Defendant asserts that the Kroll Report and related communications between Kroll and Defendant are protected by the attorney-client privilege. (Def's 6/15 Letter, at 2). This privilege attaches to “(1) a communication (2) made between privileged persons (3) in confidence (4) for the purpose of obtaining or providing legal assistance for the client.”

In re Teleglobe Commc'ns Corp., 493 F.3d 345, 359 (3d Cir. 2007) (internal quotation marks omitted), as amended (Oct. 12, 2007). “ ‘Privileged persons’ include the client, the attorney(s), and any of their agents that help facilitate attorney-client communications or the legal representation.”

Teleglobe, 493 F.3d at 359 (citing Restatement (3d) Lawyers § 70).

Because “the attorney-client privilege obstructs the truth-finding process, it is construed narrowly.” Westinghouse Elec. Corp. v. Republic of the Philippines, 951 F.2d 1414, 1423 (3d Cir. 1991). “A communication is only privileged if it is made ‘in confidence.’ ” Teleglobe, 493 F.3d at 361 (citing Restatement (3d) Lawyers § 68). Where “persons other than the client, its attorney, or their agents are present, the communication is not made in confidence, and the privilege does not attach.” Teleglobe, 493 F.3d at 361. However, “[a]s a general matter, the privilege is not destroyed when a person other than the lawyer is present at a conversation between an attorney and his or her client if that person is needed to make the conference possible or to assist the attorney in providing legal services.” Miller v. Haulmark Transp. Sys., 104 F.R.D. 442, 445 (E.D. Pa. 1984) (privilege not waived by presence of insurance agent who arranged coverage and aided in preparation of answer); see also Quaglarello v. Dewees, 802 F.Supp.2d 620, 632-33 (E.D. Pa. 2011) (finding no waiver of attorney-client privilege where 18-year-old student-plaintiff consulted with her lawyer in the presence of her parents and a neighbor who facilitated her obtaining legal counsel);

Harkobusic v. Gen. Am. Transp. Corp., 31 F.R.D. 264, 266 (W.D. Pa. 1962) (holding attorney-client privilege applied to communications between client's brother-in-law and various attorneys where brother-in-law was acting as client's agent in seeking legal advice). “These exceptions are consistent with the goal underlying the privilege because [this] type of disclosure is sometimes necessary for the client to obtain informed legal advice.”

Westinghouse, 951 F.2d at 1424.

*4 A communication may only be privileged if its primary purpose is to gain or provide legal assistance. Kramer v. Raymond Corp., 1992 WL 122856, at *1 (E.D. Pa. 1992). The attorney or agent must be “ ‘acting as a lawyer’ – giving advice with respect to the legal implications of a proposed course of conduct.” Hercules Inc. v. Exxon Corp., 434 F.Supp. 136, 147 (D. Del. 1977). For the assistance to be ‘legal’ in nature, the lawyer must guide future conduct by interpreting and applying legal principles to specific facts. PAUL R. RICE, ATTORNEY-CLIENT PRIVILEGE IN THE UNITED STATES. § 7:10 (2019). The primary purpose of each communication deemed privileged must be to gain or provide legal assistance. Kramer, 1992 WL 122856, at *1. “Merely because a legal issue can be identified that relates to on-going communications does not justify shielding them from discovery.” In re Vioxx Products Liability Litigation, 501 F. Supp. 2d 789, 798 (E.D. La. 2007). Importantly, the attorney-client privilege does not protect the communication of facts. Upjohn Co. v. United States, 449 U.S. 383, 395-96 (1981) (“The client cannot be compelled to answer the question, ‘what did you say or write to the attorney?’ but may not refuse to disclose any relevant fact within his knowledge merely because he incorporated a statement of such fact into his communication to his attorney.”); U.S. Fidelity & Guar. Co. v. Barron Industries, Inc., 809 F.Supp. 355, 364 (M.D. Pa. 1992) (“The privilege simply does not attach to a discussion of the facts, no matter how extensive or involved the discussion may become.”).

Here, Defendant does not establish that the Kroll Report and related communications involved “presenting opinions and setting forth ... tactics” rather than discussing facts. See Fidelity & Guar. Co., 809 F.Supp. at 364. The SOW shows that Kroll was employed to collect data from Defendant's equipment, to monitor Defendant's equipment, to determine
whether Defendant's equipment was compromised and to what extent, and to “work alongside Rutter's IT personnel to identify and remediate any potential vulnerabilities.” (Def's 6/15 Letter, at 14). Only one portion of this description of services is not inherently factual: Kroll's role in working with Rutter's IT personnel to identify and remediate potential vulnerabilities. (Def's 6/15 Letter, at 14). However, this service cannot be deemed to be gaining or providing legal assistance, as neither Kroll nor Rutter's IT personnel are professionals in the field of law and this service involves those two entities working alongside each other with no mention of attorney involvement. (Def's 6/15 Letter, at 14); see Kramer, 1992 WL 122856, at *1.

For the foregoing reasons, Defendant does not carry its burden of establishing that the Kroll Report and related communications between Kroll and Defendant had a primary purpose of providing or obtaining legal assistance for Defendant. See Teleglobe, 493 F.3d at 359. The record shows that the report and communications were either factual in nature or, where advice and tactics were involved, did not include legal input. (Def's 6/15 Letter, at 14); see Teleglobe, 493 F.3d at 359. The attorney-client privilege does not apply to the Kroll Report and related communications between Kroll and Defendant.

C. CONCLUSION

For the foregoing reasons, Plaintiffs' motion to compel production of the Kroll report and related communications between Kroll and Defendant is granted, and Defendant is to produce the same to Plaintiffs within 14 days of the date of this Order.

All Citations

Slip Copy, 2021 WL 3733137

Footnotes

1 “A reasonable anticipation of litigation is not established by the mere fact litigation occurred, the party consulted or retained an attorney, undertook an investigation, or engaged in negotiations.” Faloney v. Wachovia Bank, N.A., 254 F.R.D. 204, 214 (E.D. Pa. 2008).

2 Frazer, Vice President of Technology at Rutter's, declares that the Kroll Report would have been prepared in a substantially different form, and may not have been necessary, had the threat of litigation or the legal obligation to notify anyone potentially affected by the incident not existed. (Def's 6/15 Letter, at 7). Litigation, alone, must form the basis of “work product,” so this declaration – in which Frazer speaks to Rutter's notification obligations as a potential basis for the report – does not establish the report as work product. (Def's 6/15 Letter, at 7); see Fed. R. Civ. P. 26(b)(3); see also Litigation, Black's Law Dictionary 11th ed. 2019) (“The process of carrying on a lawsuit.”).
COVID-19 Vaccines

Vaccine appointments are available at New York State mass vaccination sites for children ages 5-11. Vaccines are also widely available through your child's pediatrician, family physician, local county health department, FQHC, or pharmacy.

FIND PROVIDER  

Department of Financial Services

Press Release

April 27, 2021

DFS ISSUES REPORT ON THE SOLARWINDS SUPPLY CHAIN ATTACK

Report Finds that DFS-regulated Companies Responded Quickly to the Attack

Report Identifies Key Cybersecurity Measures to Reduce Supply Chain Risk

The New York State Department of Financial Services (“the Department” or “DFS”) today released a report on the Department's investigation of the New York’s financial services industry's response to the supply chain attack of the information technology ("IT") company SolarWinds (“the SolarWinds Attack”). During the SolarWinds Attack, hackers corrupted routine
Reports and Publications

to thousands of organizations’ information

“This incident confirms that the next great financial crisis could come from a cyber attack,” said Superintendent of Financial Services Linda A. Lacewell. “Seeing hackers get access to thousands of organizations in one stroke underscores that cyber attacks threaten not just individual companies but also the stability of the financial industry as a whole.”

The report summarizes the SolarWinds Attack, the response by DFS-regulated companies, and key measures to prevent or mitigate against future supply chain attacks.

The Department found that DFS-regulated companies generally responded quickly. For example, 94% of the reporting companies removed the vulnerabilities from their IT systems within three days of the SolarWinds Attack’s announcement. However, the Department also found that some companies were not applying patches as regularly as needed to ensure timely remediation of high-risk cyber exposure.

In the report, DFS identifies the following cybersecurity measures as critical practices:

- Fully assess and address third party risk.
- Adopt a “zero trust” approach and implement multiple layers of security.
- Timely address vulnerabilities through patch deployment, testing, and validation.
- Address supply chain compromise in incident response plans.

The report furthers DFS’s commitment to improving cybersecurity and sharing information to protect consumers and the industry. DFS has also issued multiple alerts regarding ongoing cyber threats, including the SolarWinds Attack, weaknesses in Microsoft Exchange Server, and an ongoing cyber fraud campaign identified by the Department.

DFS’s first-in-the-nation Cybersecurity Regulation took effect in March 2017. DFS’s Cybersecurity Regulation has served as a model for other regulators, including the U.S. Federal Trade Commission, multiple states, the National Association of Insurance Commissioners, and the Conference of State Bank Supervisors. In 2019, DFS was also the first financial services regulator to create a Cybersecurity Division to oversee all aspects of its Cybersecurity Regulation across New York’s financial services industry.

A copy of the report can be found on the DFS website.

###
COVID-19 Vaccines

Vaccine appointments are available at New York State mass vaccination sites for children ages 5-11. Vaccines are also widely available through your child's pediatrician, family physician, local county health department, FQHC, or pharmacy.

FIND PROVIDER

Industry Guidance

From: Cybersecurity Division, Department of Financial Services
Re: Microsoft Reports Exploitation of Four Vulnerabilities in Microsoft Exchange Server
Date: March 9, 2021

In recent days, thousands of organizations were compromised via zero-day vulnerabilities in Microsoft Exchange Server. On March 2, 2021, Microsoft made patches available for these vulnerabilities but many organizations were compromised either before the patches were available or before the patches were applied.

The Department of Financial Services (“DFS”) urges all regulated entities with vulnerable Microsoft Exchange services to act immediately. Regulated entities should immediately patch or disconnect vulnerable servers, and use the tools provided by Microsoft to identify and remediate any compromise exploiting these zero-day vulnerabilities. The U.S. Department of Homeland Security Cybersecurity & Infrastructure Security Agency (“CISA”) has also released a current activity update outlining how to search for a compromise.

Background: On March 2, 2021, Microsoft reported that four vulnerabilities were discovered in the Microsoft Exchange servers from 2013 and later (including 2016, 2019). The vulnerable servers appear to host Web versions of Microsoft’s email program Outlook on their own
machines instead of cloud providers. It also appears that the vulnerabilities were being exploited for some time before March 2, and that widespread exploitation of the vulnerabilities is ongoing.

On March 2nd Microsoft also released several security updates for vulnerabilities affecting the on-premises versions of Microsoft Exchange Server. The Common Vulnerabilities and Exposures (“CVE”) exploited were CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065. Microsoft stated that these exploits “require[] the ability to make an untrusted connection to Exchange server port 443. This can be protected against by restricting untrusted connections or by setting up a VPN to separate the Exchange server from external access.” The other vulnerabilities that were also fixed in the March 2nd updates were CVE-2021-26412, CVE-2021-26854, and CVE-2021-27078 and, according to Microsoft, are “not related to known attacks.”

**CISA Recommendations:** As of March 5, 2021, CISA Emergency Directive 21-02: Mitigate Microsoft Exchange On-Premises Product Vulnerabilities recommends immediate patching of the vulnerabilities and preserving forensics of the cyber event. CISA reported that the threat actors deployed web shells on the compromised servers to establish persistent access to the victims network. Web shells can allow attackers to steal data and perform additional malicious actions, installing the patches alone will not remove malicious web shells that were deployed before patching. We therefore recommend carefully considering the steps proposed in the CISA Emergency Directive to identify exploited servers and find web shells. We recommend reviewing the following resources:

- Microsoft Advisory: Multiple Security Updates Released for Exchange Server
- Microsoft Blog: HAFNIUM targeting Exchange Servers with 0-day exploits
- Microsoft GitHub Repository: CSS-Exchange
- CISA Alert (AA21-062A): Mitigate Microsoft Exchange Server Vulnerabilities

Regulated entities should immediately assess the risk to their systems and consumers, and take steps necessary to address vulnerabilities and customer impact. The assessment should identify internal use of vulnerable Microsoft Exchange products and any use of these products by critical third parties. Regulated entities should also continue to track developments in this compromise and respond quickly to new information.

Regulated entities are reminded to report Cybersecurity Events pursuant to 23 NYCRR Section 500.17(a) as promptly as possible and within 72 hours at the latest.

Any questions or comments regarding this Alert should be directed to CyberAlert@dfs.ny.gov.
Common Vulnerabilities and Exposures ("CVE") records or numbers are unique, common identifiers for publicly known cybersecurity vulnerabilities. See The Mitre Organization, "About CVE Records."

Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments

Date: September 21, 2021

The U.S. Department of the Treasury’s Office of Foreign Assets Control (OFAC) is issuing this updated advisory to highlight the sanctions risks associated with ransomware payments in connection with malicious cyber-enabled activities and the proactive steps companies can take to mitigate such risks, including actions that OFAC would consider to be “mitigating factors” in any related enforcement action.2

Demand for ransomware payments has increased during the COVID-19 pandemic as cyber actors target online systems that U.S. persons rely on to continue conducting business. Companies that facilitate ransomware payments to cyber actors on behalf of victims, including financial institutions, cyber insurance firms, and companies involved in digital forensics and incident response, not only encourage future ransomware payment demands but also may risk violating OFAC regulations. The U.S. government strongly discourages all private companies and citizens from paying ransom or extortion demands and recommends focusing on strengthening defensive and resilience measures to prevent and protect against ransomware attacks.

This advisory describes the potential sanctions risks associated with making and facilitating ransomware payments and provides information for contacting relevant U.S. government agencies, including OFAC if there is any reason to suspect the cyber actor demanding ransomware payment may be sanctioned or otherwise have a sanctions nexus.3

Background on Ransomware Attacks

Ransomware is a form of malicious software (“malware”) designed to block access to a computer system or data, often by encrypting data or programs on information technology systems to extort ransom payments from victims in exchange for decrypting the information and restoring victims’ access to their systems or data. In some cases, in addition to the attack, cyber actors threaten to publicly disclose victims’ sensitive files. The cyber actors then demand a

---

1 This advisory is explanatory only and does not have the force of law. It does not modify statutory authorities, Executive Orders, or regulations. It is not intended to be, nor should it be interpreted as, comprehensive, or as imposing requirements under U.S. law, or otherwise addressing any requirements under applicable law. Please see the legally binding provisions cited for relevant legal authorities.

2 This advisory updates and supersedes OFAC’s Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments of October 1, 2020.

3 This advisory is limited to sanctions risks related to ransomware and is not intended to address issues related to information security practitioners’ cyber threat intelligence-gathering efforts more broadly. For guidance related to those activities, see guidance from the U.S. Department of Justice, Legal Considerations when Gathering Online Cyber Threat Intelligence and Purchasing Data from Illicit Sources (February 2020), available at https://www.justice.gov/criminal-ccips/page/file/1252341/download.
ransomware payment, usually through virtual currency, in exchange for a key to decrypt the files and restore victims’ access to systems or data.

In recent years, ransomware attacks have become more focused, sophisticated, costly, and numerous. According to the Federal Bureau of Investigation (FBI), there was a nearly 21 percent increase in reported ransomware cases and a 225 percent increase in associated losses from 2019 to 2020. Ransomware attacks are carried out against private and governmental entities of all sizes and in all sectors, including organizations operating critical infrastructure, such as hospitals. Often attacks also take place against vulnerable entities such as school districts and smaller businesses, in part due to the attacker’s assumption that such victims may have fewer resources to invest in cyber protection and will make quick payment to restore services.

**OFAC Designations of Malicious Cyber Actors**

OFAC has designated numerous malicious cyber actors under its cyber-related sanctions program and other sanctions programs, including perpetrators of ransomware attacks and those who facilitate ransomware transactions. For example, starting in 2013, a ransomware variant known as Cryptolocker was used to infect more than 234,000 computers, approximately half of which were in the United States. OFAC designated the developer of Cryptolocker, Evgeniy Mikhailovich Bogachev, in December 2016.

Starting in late 2015 and lasting approximately 34 months, SamSam ransomware was used to target mostly U.S. government institutions and companies, including the City of Atlanta, the Colorado Department of Transportation, and a large healthcare company. In November 2018, OFAC designated two Iranians for providing material support to a malicious cyber activity and identified two virtual currency addresses used to funnel SamSam ransomware proceeds.

In May 2017, a ransomware known as WannaCry 2.0 infected approximately 300,000 computers in at least 150 countries. This attack was linked to the Lazarus Group, a cybercriminal organization sponsored by North Korea. OFAC designated the Lazarus Group and two subgroups, Bluenoroff and Andariel, in September 2019.

---


Beginning in 2015, Evil Corp, a Russia-based cybercriminal organization, used the Dridex malware to infect computers and harvest login credentials from hundreds of banks and financial institutions in over 40 countries, causing more than $100 million in theft. In December 2019, OFAC designated Evil Corp and its leader, Maksim Yakubets, for their development and distribution of the Dridex malware.\(^9\)

In September 2021, OFAC designated SUEX OTC, S.R.O. (“SUEX”), a virtual currency exchange, for its part in facilitating financial transactions for ransomware actors, involving illicit proceeds from at least eight ransomware variants. Analysis of known SUEX transactions showed that over 40% of SUEX’s known transaction history was associated with illicit actors.\(^10\)

OFAC has imposed, and will continue to impose, sanctions on these actors and others who materially assist, sponsor, or provide financial, material, or technological support for these activities.\(^11\)

**Ransomware Payments with a Sanctions Nexus Threaten U.S. National Security Interests**

Facilitating a ransomware payment that is demanded as a result of malicious cyber activities may enable criminals and adversaries with a sanctions nexus to profit and advance their illicit aims. For example, ransomware payments made to sanctioned persons or to comprehensively sanctioned jurisdictions could be used to fund activities adverse to the national security and foreign policy objectives of the United States. Such payments not only encourage and enrich malicious actors, but also perpetuate and incentivize additional attacks. Moreover, there is no guarantee that companies will regain access to their data or be free from further attacks themselves. For these reasons, the U.S. government strongly discourages the payment of cyber ransom or extortion demands.

**Facilitating Ransomware Payments on Behalf of a Victim May Violate OFAC Regulations**

Under the authority of the International Emergency Economic Powers Act (IEEPA) or the Trading with the Enemy Act (TWEA),\(^12\) U.S. persons are generally prohibited from engaging in transactions, directly or indirectly, with individuals or entities (“persons”) on OFAC’s Specially Designated Nationals and Blocked Persons List (SDN List), other blocked persons, and those covered by comprehensive country or region embargoes (e.g., Cuba, the Crimea region of

---


Ukraine, Iran, North Korea, and Syria). Additionally, any transaction that causes a violation under IEEPA, including a transaction by a non-U.S. person that causes a U.S. person to violate any IEEPA-based sanctions prohibitions, is also prohibited. U.S. persons, wherever located, are also generally prohibited from facilitating actions of non-U.S. persons that could not be directly performed by U.S. persons due to U.S. sanctions regulations.

OFAC may impose civil penalties for sanctions violations based on strict liability, meaning that a person subject to U.S. jurisdiction may be held civilly liable even if such person did not know or have reason to know that it was engaging in a transaction that was prohibited under sanctions laws and regulations administered by OFAC. OFAC’s Economic Sanctions Enforcement Guidelines (Enforcement Guidelines) provide more information regarding OFAC’s enforcement of U.S. economic sanctions, including the factors that OFAC generally considers when determining an appropriate response to an apparent violation. Enforcement responses range from non-public responses, including issuing a No Action Letter or a Cautionary Letter, to public responses, such as civil monetary penalties.

**Sanctions Compliance Program and Defensive/Resilience Measures**

Under OFAC’s Enforcement Guidelines, the existence, nature, and adequacy of a sanctions compliance program is a factor that OFAC may consider when determining an appropriate enforcement response to an apparent violation of U.S. sanctions laws or regulations.

As a general matter, OFAC encourages financial institutions and other companies to implement a risk-based compliance program to mitigate exposure to sanctions-related violations. This also applies to companies that engage with victims of ransomware attacks, such as those involved in providing cyber insurance, digital forensics and incident response, and financial services that may involve processing ransom payments (including depository institutions and money services businesses). In particular, the sanctions compliance programs of these companies should account for the risk that a ransomware payment may involve an SDN or blocked person, or a comprehensively embargoed jurisdiction. Companies involved in facilitating ransomware payments on behalf of victims should also consider whether they have regulatory obligations under Financial Crimes Enforcement Network (FinCEN) regulations.

Meaningful steps taken to reduce the risk of extortion by a sanctioned actor through adopting or improving cybersecurity practices, such as those highlighted in the Cybersecurity and Infrastructure Security Agency’s (CISA) September 2020 Ransomware Guide, will be

---

13 31 C.F.R. part 501, appx. A.
14 To assist the public in developing an effective sanctions compliance program, in 2019, OFAC published A Framework for OFAC Compliance Commitments, intended to provide organizations with a framework for the five essential components of a risk-based sanctions compliance program. The Framework is available at https://home.treasury.gov/system/files/126/framework_ofac_cc.pdf.
15 See FinCEN Guidance, FIN-2020-A006, Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments, October 1, 2020, for applicable anti-money laundering obligations related to financial institutions in the ransomware context.
considered a significant mitigating factor in any OFAC enforcement response. Such steps could include maintaining offline backups of data, developing incident response plans, instituting cybersecurity training, regularly updating antivirus and anti-malware software, and employing authentication protocols, among others.

Cooperation with OFAC and Law Enforcement

Another factor that OFAC will consider under the Enforcement Guidelines is the reporting of ransomware attacks to appropriate U.S. government agencies and the nature and extent of a subject person’s cooperation with OFAC, law enforcement, and other relevant agencies, including whether an apparent violation of U.S. sanctions is voluntarily self-disclosed. In the case of ransomware payments that may have a sanctions nexus, OFAC will consider a company’s self-initiated and complete report of a ransomware attack to law enforcement or other relevant U.S. government agencies, such as CISA or the U.S. Department of the Treasury’s Office of Cybersecurity and Critical Infrastructure Protection (OCCIP), made as soon as possible after discovery of an attack, to be a voluntary self-disclosure and a significant mitigating factor in determining an appropriate enforcement response. OFAC will also consider a company’s full and ongoing cooperation with law enforcement both during and after a ransomware attack — e.g., providing all relevant information such as technical details, ransom payment demand, and ransom payment instructions as soon as possible — to be a significant mitigating factor.

While the resolution of each potential enforcement matter depends on the specific facts and circumstances, OFAC would be more likely to resolve apparent violations involving ransomware attacks with a non-public response (i.e., a No Action Letter or a Cautionary Letter) when the affected party took the mitigating steps described above, particularly reporting the ransomware attack to law enforcement as soon as possible and providing ongoing cooperation.

OFAC Licensing Policy

Ransomware payments benefit illicit actors and can undermine the national security and foreign policy objectives of the United States. For this reason, license applications involving ransomware payments demanded as a result of malicious cyber-enabled activities will continue to be reviewed by OFAC on a case-by-case basis with a presumption of denial.

Victims of Ransomware Attacks Should Contact Relevant Government Agencies

OFAC strongly encourages all victims and those involved with addressing ransomware attacks to report the incident to CISA, their local FBI field office, the FBI Internet Crime Complaint Center, or their local U.S. Secret Service office as soon as possible. Victims should also report ransomware attacks and payments to Treasury’s OCCIP and contact OFAC if there is any reason to suspect a potential sanctions nexus with regard to a ransomware payment. As noted, in doing so victims can receive significant mitigation from OFAC when determining an appropriate enforcement response in the event a sanctions nexus is found in connection with a ransomware payment.

---

17 See the U.S. government's website, https://www.cisa.gov/stopransomware, for additional guidance.
By reporting ransomware attacks as soon as possible, victims may also increase the likelihood of recovering access to their data through other means, such as alternative decryption tools, and in some circumstances may be able to recover some of the ransomware payment. Additionally, reporting ransomware attacks and payments provides critical information needed to track cyber actors, hold them accountable, and prevent or disrupt future attacks.

Contact Information for U.S. Department of Treasury Agencies:

- U.S. Department of the Treasury’s Office of Foreign Assets Control
  - Sanctions Compliance and Evaluation Division: ofac_feedback@treasury.gov; (202) 622-2490 / (800) 540-6322
  - Licensing Division: https://licensing.ofac.treas.gov; (202) 622-2480
- U.S. Department of the Treasury’s Office of Cybersecurity and Critical Infrastructure Protection (OCCIP)
  - OCCIP-Coord@treasury.gov; (202) 622-3000
- U.S. Department of the Treasury’s Financial Crimes Enforcement Network (FinCEN)
  - FinCEN Regulatory Support Section: frc@fincen.gov

Contact Information for Other Relevant U.S. Government Agencies:

- Federal Bureau of Investigation Cyber Task Force
- U.S. Secret Service Cyber Fraud Task Force
  - https://secretservice.gov/contact/field-offices
- Cybersecurity and Infrastructure Security Agency
  - https://us-cert.cisa.gov/forms/report
- Homeland Security Investigations Field Office
  - https://www.ice.gov/contact/hsi

Ransomware Prevention Resources:

- U.S. Government StopRansomWare.gov Website
  - https://www.cisa.gov/stopransomware
- CISA Ransomware Guide
  - https://www.cisa.gov/stopransomware/ransomware-guide

If you have any questions regarding the scope of any sanctions requirements described in this advisory, please contact OFAC’s Sanctions Compliance and Evaluation Division at (800) 540-6322 or (202) 622-2490.

381 F.Supp.3d 1240
United States District Court, E.D. California.

UNITED STATES of America
ex rel. Brian Markus, Plaintiff,
v.
AEROJET ROCKETDYNE HOLDINGS,
INC., a corporation and Aerojet Rocketdyne,
Inc., a corporation, Defendants.

No. 2:15-cv-2245 WBS AC
Signed May 8, 2019

Synopsis

Background: Relator brought action against employer arising from employer's allegedly wrongful conduct in violation of False Claims Act (FCA), and relating to employer's termination of relator's employment. Defendants moved to dismiss in part for failure to state claim, to stay proceedings, and compel arbitration.

Holdings: The District Court, William B. Shubb, J., held that:

[1] relator stated claims alleging promissory fraud or false or fraudulent statement or record, in violation of FCA;

[2] relator failed to state conspiracy claim under FCA; and

[3] it was not appropriate to expand stay of relator's employment-related claims, and referral of those claims to arbitration, to include relator's FCA claims.

Ordered accordingly.

Procedural Posture(s): Motion to Dismiss for Failure to State a Claim; Motion to Stay Proceedings; Motion to Compel Arbitration.

West Headnotes (20)

[1] Federal Civil Procedure ⇆ Insufficiency in general
A claim has “facial plausibility,” as required to overcome motion to dismiss for failure to state a claim, when the plaintiff pleads factual content that allows the court to draw the reasonable inference the defendant is liable for the misconduct alleged. Fed. R. Civ. P. 12(b)(6).

A complaint that offers mere labels and conclusions will not survive a motion to dismiss for failure to state a claim. Fed. R. Civ. P. 12(b)(6).

[3] United States ⇆ False certification
Under a false certification theory of fraud under False Claims Act (FCA), relator can allege either express or implied false certification; express false certification requires that claimant plainly and directly certify its compliance with certain requirements that it has breached, whereas implied false certification can be a basis for liability where claim does not merely request payment, but also makes specific representations about the goods or services provided, and defendant's failure to disclose noncompliance with material statutory, regulatory, or contractual requirements makes those representations misleading half-truths.

1 Cases that cite this headnote

The promissory fraud approach under False Claims Act (FCA) attaches liability to each claim submitted to the government under a contract, when the contract or extension of government benefit was originally obtained through false statements or fraudulent conduct.

Under either false certification or promissory fraud theory, the essential elements of False Claims Act (FCA) liability remain the same: (1) a false statement or fraudulent course of conduct; (2) made with scienter; (3) that was material; causing (4) the government to pay out money or forfeit moneys due. 31 U.S.C.A. §§ 3729(a)(1)(A), 3729(a)(1)(B).

Allegations that employer did not fully disclose extent of its computer systems' noncompliance with Department of Defense rules requiring defense contractors to safeguard unclassified controlled technical information from cybersecurity threats, as well as National Aeronautics and Space Administration (NASA) acquisition regulations governing security requirements for contractors, when entering into missile defense and rocket engine technology contracts with government were sufficient to allege employer made material falsehoods as to its noncompliance with rules, as required to state claims alleging promissory fraud or false or fraudulent statement or record, in violation of False Claims Act (FCA). 31 U.S.C.A. §§ 3729(a)(1)(A), 3729(a)(1)(B).

1 Cases that cite this headnote

A relator's False Claims Act (FCA) claims must not only be plausible but pled with particularity under Federal Rule of Civil Procedure governing pleading of fraud allegations. 31 U.S.C.A. § 3729; Fed. R. Civ. P. 9(b).

[7] United States Materiality
The materiality of falsehood under False Claims Act (FCA) looks to the effect on the behavior of the recipient of the alleged misrepresentation. 31 U.S.C.A. § 3729(b)(4).

[8] United States Materiality
A misrepresentation is not material, for purposes of False Claims Act (FCA), simply because the government requires compliance with certain requirements as a condition of payment. 31 U.S.C.A. § 3729(b)(4).

[9] United States Materiality
A court cannot find materiality for purposes of False Claims Act (FCA) claim where the government would have the option to decline to pay if it knew of the defendant's noncompliance. 31 U.S.C.A. § 3729(b)(4).

[10] United States Materiality


[12] Evidence Official proceedings and acts
District Court would take judicial notice of publications on government websites, as well as authorization to operate signed by National Aeronautics and Space Administration (NASA) officials. Fed. R. Evid. 201(b)(2).

[13] United States Materiality
If relators' ability to plead sufficiently the element of materiality in False Claims Act (FCA) proceeding were stymied by the government's choice not to intervene, this would undermine the purposes of the FCA, as it allows relators to proceed even without government intervention. 31 U.S.C.A. § 3729(b)(4).
[14] United States ➞ Materiality

When evaluating materiality as part of False Claims Act (FCA) claim, courts should consider how the government has treated similar violations. 31 U.S.C.A. § 3729(b)(4).

[15] Conspiracy ➞ Intracorporate conspiracy doctrine in general

The “intracorporate conspiracy doctrine” states that a conspiracy requires an agreement among two or more persons or distinct business entities. 31 U.S.C.A. § 3729(b)(4).

[16] Conspiracy ➞ Fraud against government; false claims

Relator failed to allege that parent company and its wholly-owned subsidiary conspired with any independent individual or entity to defraud United States by knowingly submitting false claims and, thus, failed to state conspiracy claim under False Claims Act (FCA). 31 U.S.C.A. § 3729(a)(1)(C).

[20] Alternative Dispute Resolution ➞ Particular cases

It was not appropriate to expand stay of relator's employment-related claims, and referral of those claims to arbitration, to include relator's claims arising under False Claims Act (FCA); FCA claims concerned fraud that employer allegedly perpetrated on government, whereas employment-based claims concerned alleged violations of relator's own rights during his employment. 9 U.S.C.A. § 3; 31 U.S.C.A. § 3729.

Attorneys and Law Firms

*1243 Gregory Anderson Thyberg, ThybergLaw, Sacramento, CA, Plaintiff.

Ashley Neglia, Mark Charles Holscher, Kirkland & Ellis LLP, Los Angeles, CA, for Defendants.

MEMORANDUM & ORDER RE: DEFENDANTS' MOTION TO DISMISS RELATOR'S SECOND AMENDED COMPLAINT, STAY PROCEEDINGS, and COMPEL ARBITRATION

WILLIAM B. SHUBB, UNITED STATES DISTRICT JUDGE

Plaintiff-relator Brian Markus brings this action against defendants Aerojet Rocketdyne Holdings, Inc. (“ARH”) and Aerojet Rocketdyne, Inc. (“AR”), arising from defendants' allegedly wrongful conduct in violation of the False Claims Act (“FCA”), 31 U.S.C. §§ 3729 et seq., and relating to
defendants’ termination of relator’s employment. Defendants now move to (1) dismiss the Second Amended Complaint (“SAC”) in part for the failure to state upon which can be granted under Federal Rule of Civil Procedure 12(b)(6), (2) stay proceedings, and (3) compel arbitration.

I. Background
Relator Brian Markus is resident of the State of California. (SAC ¶ 6 (Docket No. 42).) He worked for defendants as the senior director of Cyber Security, Compliance, and Controls from June 2014 to September 2015. (Id.) Defendants ARH and AR develop and manufacture products for the aerospace and defense industry. (Id. ¶ 7.) Defendants’ primary aerospace and defense customers include the Department of Defense (“DoD”) and the National Aeronautics & Space Administration (“NASA”), who purchase defendants’ products pursuant to government contracts. (See id.) Defendant AR is a wholly-owned subsidiary of ARH, and ARH uses AR to perform its contractual obligations. (Id. ¶ 8.)

Government contracts are subject to Federal Acquisition Regulations and are supplemented by agency specific regulations. On November 18, 2013, the DoD issued a final rule, which imposed requirements on defense contractors to safeguard unclassified controlled technical information from cybersecurity threats. 48 C.F.R. § 252.204-7012 (2013). The rule required defense contractors to implement specific controls covering many different areas of cybersecurity, though it did allow contractors to submit an explanation to federal officers explaining how the company had alternative methods for achieving adequate cybersecurity protection, or why standards were inapplicable. See id. In August 2015, the DoD issued an interim rule, modifying the government’s cybersecurity requirements for contractor and subcontractor information systems. 48 C.F.R. § 252.204-7012 (Aug. 2015). The interim rule incorporated more cybersecurity controls and required *1244 that any alternative measures be “approved in writing prior by an authorized representative of the DoD [Chief Information Officer] prior to contract award.” Id. at 252.204-7012(b)(1)(ii)(A). The DoD amended the interim rule in December 2015 to allow contractors until December 31, 2017 to have compliant or equally effective alternative controls in place. See 48 C.F.R. § 252.204-7012(b)(1)(ii)(A) (Dec. 2015). Each version of this regulation defines adequate security as “protective measures that are commensurate with the consequences and probability of loss, misuse, or unauthorized access to, or modification of information.” 48 C.F.R. § 252.204–7012(a).

Contractors awarded contracts from NASA must comply with relevant NASA acquisition regulations. 48 C.F.R. § 1852.204-76 lists the relevant security requirements where a contractor stores sensitive but unclassified information belonging to the federal government. Unlike the relevant DoD regulation, this NASA regulation makes no allowance for the contractor to use alternative controls or protective measures. A NASA contractor is required to “protect the confidentiality, integrity, and availability of NASA Electronic Information and IT resources and protect NASA Electronic Information from unauthorized disclosure.” 48 C.F.R. § 1852.204-76(a).

Relator alleges that defendants fraudulently entered into contracts with the federal government despite knowing that they did not meet the minimum standards required to be awarded a government contract. (SAC ¶ 30.) He alleges that when he started working for defendants in 2014, he found that defendants’ computer systems failed to meet the minimum cybersecurity requirements to be awarded contracts funded by the DoD or NASA. (Id. ¶ 36.) He claims that defendants knew AR was not compliant with the relevant standards as early as 2014, when defendants engaged Emagined Security, Inc. to audit the company’s compliance. (See id. at ¶¶ 43, 51-53.) Relator avers that defendants repeatedly misrepresented its compliance with these technical standards in communications with government officials. (Id. ¶ 59-64.)

Relator alleges that the government awarded AR a contract based on these allegedly false and misleading statements. (Id. ¶ 65.) In July 2015, relator refused to sign documents that defendants were now compliant with the cybersecurity requirements, contacted the company’s ethics hotline, and filed an internal report. (Id. ¶¶ 81-82.) Defendants terminated relator’s employment on September 14, 2015. (Id. ¶ 83.)

Relator filed his initial complaint in this action on October 29, 2015. (Docket No. 1.) While the government was still deciding whether to intervene in this action, relator filed his First Amended Complaint (“FAC”) on September 13, 2017. (Docket No. 22.) On June 5, 2018, the United States filed a notice of election to decline intervention. (Docket No. 25.) A few months later defendants filed a motion to dismiss, stay proceedings, and compel arbitration as to the FAC. (Docket No. 39.) In response to this motion, relator filed the SAC, alleging the following causes of action against defendants: (1) promissory fraud in violation of 31 U.S.C. § 3729(a)(1)(A); (2) false or fraudulent statement or record in violation of 31 U.S.C. § 3729(a)(1)(B); (3) conspiracy to submit false claims in violation of 31 U.S.C. § 3729(a)(1)(C); (4)
II. Motion to Dismiss

A. Legal Standard

[1] [2] On a Rule 12(b)(6) motion, the inquiry before the court is whether, accepting the allegations in the complaint as true and drawing all reasonable inferences in the plaintiff's favor, the plaintiff has stated a claim to relief that is plausible on its face. See Ashcroft v. Iqbal, 556 U.S. 662, 678, 129 S.Ct. 1937, 173 L.Ed.2d 868 (2009). “The plausibility standard is not akin to a ‘probability requirement,’ but it asks for more than a sheer possibility that a defendant has acted unlawfully.” Id. “A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged.” Id. A complaint that offers mere “labels and conclusions” will not survive a motion to dismiss. Id. (internal quotation marks and citations omitted).

B. Fraud Claims under the FCA

Relator brings two claims for fraud under the FCA. These two claims impose liability on anyone who “knowingly presents, or causes to be presented, a false or fraudulent claim for payment or approval,” 31 U.S.C. § 3729(a)(1)(A), or “knowingly makes, uses, or causes to be made or used, a false record or statement material to a false or fraudulent claim,” id. § 3729(a)(1)(B).

[3] [4] Outside of the context where “the claim for payment is itself literally false or fraudulent,” the Ninth Circuit recognizes two different doctrines that attach FCA liability to allegedly false or fraudulent claims: (1) false certification and (2) promissory fraud, also known as fraud in the inducement. See United States ex rel. Hendow v. Univ. of Phoenix, 461 F.3d 1166, 1170-71 (9th Cir. 2006) (citation omitted). Under a false certification theory, the relator can allege either express false certification or implied false certification. The express false certification theory requires that the claimant plainly and directly certify its compliance with certain requirements that it has breached. See id. An implied false certification theory “can be a basis for liability, at least where two conditions are satisfied: first, the claim does not merely request payment, but also makes specific representations about the goods or services provided; and second, the defendant's failure to disclose noncompliance with material statutory, regulatory, or contractual requirements makes those representations misleading half-truths.” Universal Health Servs., Inc. v. United States ex rel. Escobar, — U.S. ———, 136 S. Ct. 1989, 2001, 195 L.Ed.2d 348 (2016). The promissory fraud approach is broader and “holds that liability will attach to each claim submitted to the government under a contract, when the contract or extension of government benefit was originally obtained through false statements or fraudulent conduct.” Hendow, 461 F.3d at 1173.

[5] [6] Under either false certification or promissory fraud, “the essential elements of [FCA] liability remain the same: (1) a false statement or fraudulent course of conduct, (2) made with scienter, (3) that was material, causing (4) the government to pay out money or forfeit moneys due.” Id. Only the sufficiency of the complaint as to the materiality requirement is at issue on this motion. 2

[7] [8] [9] Under the FCA, a falsehood is material if it has “a natural tendency to influence, or be capable of influencing, the payment or receipt of money or property.” 31 U.S.C. § 3729(b)(4). Most recently in Escobar, the Supreme Court clarified that “[t]he materiality standard is demanding.” 136 S.Ct. at 2003. Materiality looks to the effect on the behavior of the recipient of the alleged misrepresentation. Id. at 2002. A misrepresentation is not material simply because the government requires compliance with certain requirements as a condition of payment. Id. at 2003. Nor can a court find materiality where “the Government would have the option to decline to pay if it knew of the defendant's noncompliance.” Id. Relatedly, mere “minor or insubstantial” noncompliance is not material. Id. Evidence relevant to the materiality inquiry includes the government's conduct in similar circumstances and whether the government has knowledge of the alleged noncompliance. 3

See id. Defendants puts forth four different arguments in support of their contention that relator has insufficiently pled facts as to the materiality requirement.
First, defendants argue that AR disclosed to its government customers that it was not compliant with relevant DoD and NASA regulations and therefore it is impossible for relator to satisfy the materiality prong. The Supreme Court did observe in Escobar that “if the Government pays a particular claim in full despite its actual knowledge that certain requirements were violated, that is very strong evidence that those requirements are not material.” Id. Here, however, relator properly alleges with sufficient particularity that defendants did not fully disclose the extent of AR's noncompliance with relevant regulations. See id. at 2000 (“[H]alf-truths—representations that state the truth only so far as it goes, while omitting critical qualifying information—can be actionable misrepresentations.”). For instance, relator alleges that AR misrepresented in its September 18, 2014 letter to the government the extent to which it had equipment required by the regulations (SAC ¶ 63), instituted required security controls (id. ¶¶ 60-61, 63), and possessed necessary firewalls (id. ¶ 62). Relator also alleges that these misrepresentations persisted over time, whereby AR knowingly and falsely certified compliance with security requirements when submitting invoices for its services. (Id. ¶¶ 135-36.) While it may be true that AR disclosed some of its noncompliance (see id. ¶¶ 59-64), a partial disclosure would not relieve defendants of liability where defendants failed to “disclose noncompliance with material statutory, regulatory, or contractual requirements.” See Escobar, 136 S. Ct. at 2001.

In fact, some of the evidence defendants put forth in favor of their motion to dismiss provides support for relator's allegations relevant to materiality. The DoD informed the federal contracting officer that it could not waive compliance with DoD regulations, even for an urgent contract. (SAC ¶¶ 67-68; Req. for Judicial Notice Ex. Z at 1-4.) While the contracting officer was not prohibited from awarding the contract because of AR's noncompliance, AR could not process, store, or transmit controlled technical information until it was fully compliant. (Req. for Judicial Notice Ex. Z at 1.) Still, the DoD representative believed it to “be a relatively simple matter for the contractor to become compliant” based on the disclosure letter AR sent to the contracting negotiator. (Id. at 1-2.) Yet, relator's complaint alleges possible material nondisclosures in this letter, such as AR's failure to report its status on all required controls, its alleged misstatements as to partial compliance with protection measures, and the fact that the company cherrypicked what data it chose to report. (See SAC ¶¶ 59-64.) Accepting these allegations as true, the government may not have awarded these contracts if it knew the full extent of the company's noncompliance, because how close AR was to full compliance was a factor in the government's decision to enter into some contracts.

Second, defendants contend that the government's response to the investigation into AR's representations surrounding its cybersecurity compliance undermines relator's allegations as to materiality. Both the DoD and NASA have continued to contract with AR since the government's investigation into the allegations of this complaint. (See Req. for Judicial Notice Exs. S-V (Docket Nos. 52-19, 52-20, 52-21 & 52-22).) Such evidence is not entirely dispositive on a motion to dismiss. Cf. Campie, 862 F.3d at 906 (cautioning courts not to read too much into “continued approval” by the government, albeit in a different context). Instead, the appropriate inquiry is whether AR's alleged misrepresentations were material at the time the government entered into or made payments on the relevant contracts. See Escobar, 136 S. Ct. at 2002. The contracts government agencies entered with AR after relator commenced this litigation are not at issue and possibly relate to a different set of factual circumstances. As discussed previously, relator has sufficiently alleged that AR's misrepresentations as to the extent of its noncompliance with government regulations could have affected the government's decision to enter into and pay on the contracts at issue in this case.

Defendants also argue that the government's decision not to intervene in this case indicates that the alleged misrepresentations were not material. (See Mot. to Dismiss at 3; Reply at 9.) As the Sixth Circuit has observed, in Escobar itself, the government chose not to intervene and the Supreme Court did not mention it as a factor relevant to materiality. See United States ex rel. Prather v. Brookdale Senior Living Communities, Inc., 892 F.3d 822, 836 (6th Cir. 2018) (citing 136 S. Ct. at 1998). Separately, “[i]f relators' ability to plead sufficiently the element of materiality were stymied by the government's choice not to intervene, this would undermine the purposes of the Act,” as the FCA allows relators to proceed even without government intervention. Id. (citation omitted). And finally, there is no reason
believe that the decision not to intervene is a comment on the merits of this case. See, e.g., United States ex rel. Atkins v. McInteer, 470 F.3d 1350, 1360 n.17 (11th Cir. 2006) (“In any given case, the government may have a host of reasons for not pursuing a claim.”); United States ex rel. Chandler v. Cook Cty., Ill., 277 F.3d 969, 974 n.5 (7th Cir. 2002) (“The Justice Department may have myriad reasons for permitting the private suit to go forward including limited prosecutorial resources and confidence in the relator's attorney.”).

Third, defendants argue that AR's noncompliance does not go to the central purpose of any of the contracts, as the contracts pertain to missile defense and rocket engine technology, not cybersecurity. See Escobar, 136 S. Ct. at 2004 n.5 (noting that a misrepresentation is material where it goes to the “essence of the bargain”). This argument is unavailing at this stage of the proceedings. Relator alleges that all of AR's relevant contracts with the DoD and NASA incorporated each entity's acquisition regulations. (See SAC ¶¶ 84, 105.) These acquisition regulations require that the defense contractor undertake cybersecurity specific measures before the contractor can handle certain technical information. Here, compliance with these cybersecurity requirements could have affected AR's ability to handle technical information pertaining to missile defense and rocket engine technology. (See Req. for Judicial Notice Ex. Z at 1.) Accordingly, misrepresentations as to compliance with these cybersecurity requirements could have influenced the extent to which AR could have performed the work specified by the contract.

[14] Fourth and finally, defendants argue that the government's response to the defense industry's non-compliance with these regulations as a whole weighs against a finding of materiality. When evaluating materiality, courts should “consider how the [government] has treated similar violations.” See United States ex rel. Rose v. Stephens Inst., 909 F.3d 1012, 1020 (9th Cir. 2018). Defendants contend that the DoD never expected full technical compliance because it constantly amended its acquisition regulations and promulgated guidelines that attempted to ease the burdens on the industry. This observation is not dispositive. Even if the government never expected full technical compliance, relator properly pleads that the extent to which a company was technically complaint still mattered to the government's decision to enter into a contract. (See SAC ¶¶ 66-72.) Defendants have not put forth any judicially noticeable evidence that the government paid a company it knew was noncompliant to the same extent as AR was. Therefore, this consideration does not weigh in favor of dismissal.

Accordingly, given the above considerations, relator has plausibly pled that defendants' alleged failure to fully disclose its noncompliance was material to the government's decision to enter into and pay on the relevant contracts. 8

C. Conspiracy under the FCA

Relator's third count alleges that defendants participated in a conspiracy to submit false claims in violation of 31 U.S.C. § 3729(a)(1)(C). Relator maintains that defendants and their officers conspired together to defraud the United States by knowingly submitting false claims. (See SAC ¶ 144.) Section 3729(a)(1)(C) imposes liability on a person who conspires to commit a violation of Section 3729(a)(1)(A) or Section 3729(a)(1)(B).

[15] Defendants argue that this count fails as a matter of law because relator has failed to identify two distinct entities that conspired. Derived from antitrust law, the intracorporate conspiracy doctrine “holds that a conspiracy requires an agreement among two or more persons or distinct business entities.” United States v. Hughes Aircraft Co., 20 F.3d 974, 979 (9th Cir. 1994) (internal quotation marks omitted). The doctrine stems from the definition of a conspiracy and the requirement that there be a meeting of the minds. See Hoefer v. Fluor Daniel, Inc., 92 F. Supp. 2d 1055, 1057 (C.D. Cal. 2000) (citing Fonda v. Gray, 707 F.2d 435, 438 (9th Cir. 1983)). While the Ninth Circuit has not addressed this issue, several district courts have applied the intracorporate conspiracy doctrine to FCA claims. See United States ex rel. Lupo v. Quality Assurance Servs., Inc., 242 F.Supp.3d 1020, 1027 (S.D. Cal. 2017) (collecting cases). Courts have used this principle to bar conspiracy claims where the alleged conspirators are a parent corporation and its wholly-owned subsidiary. See, e.g., United States ex rel. Campie v. Gilead Scis., Inc., No. C-11-0941 EMC, 2015 WL 106255, at *15 (N.D. Cal. Jan. 7, 2015).

[16] [17] Here, relator identifies only a parent company, ARH, and its wholly-owned subsidiary, AR, as defendants. (SAC ¶¶ 7-8.) While relator alleges that defendants also conspired with its officers, a corporation, as a matter of law, “cannot conspire with its own employees or agents.” Hoefer.
By failing to allege that defendants conspired with any independent individual or entity, relator's conspiracy claim fails as a matter of law.

Accordingly, the court will dismiss relator's third claim, that defendants participated in a conspiracy to submit false claims in violation of 31 U.S.C. § 3729(a)(1)(C).

III. Motion to Compel Arbitration and Stay Proceedings

“Relator does not oppose defendants’ motion to refer his employment related claims to arbitration” based on his arbitration agreement with defendants. (Opp'n to Mot. to Dismiss at 16 (Docket No. 53); see also Decl. of Ashley Neglia Ex. 1 (arbitration agreement) (Docket No. 51-1).) Relator does oppose, however, defendants' request that the entire proceedings be stayed pending the resolution of these employment related claims in arbitration. Relator contends that a stay is inappropriate as to his FCA claims because they are brought on behalf of the government, are not referable to arbitration, and are separate from the issues involved in his employment-related claims. (See Opp'n to Mot. to Dismiss at 16-17.)

Section 3 of the FAA provides that a court “shall on application of one of the parties stay the trial” of “any suit proceeding” brought “upon any issue referable to arbitration under [an arbitration] agreement ... until such arbitration has been had in accordance with the terms of the agreement.” 9 U.S.C. § 3. A party is only “entitled to a stay pursuant to section 3” as to arbitrable claims. Leyva v. Certified Grocers of Cal., Ltd., 593 F.2d 857, 863 (9th Cir. 1979). As to nonarbitrable claims, which defendants concede the FCA claims are, this court has discretion whether to stay the litigation pending arbitration. Id. at 863-64. This court may decide whether “it is efficient for its own docket and the fairest course for the parties to enter a stay of an action before it, pending resolution of independent proceedings which bear upon the case.” Id. at 863. If there is a fair possibility that the stay may work damage to another party, a stay may be inappropriate. See Dependable Highway Exp., Inc. v. Navigators Ins. Co., 498 F.3d 1059, 1066 (9th Cir. 2007) (citation omitted).

The court will not expand the stay to encompass the nonarbitrable FCA claims. The issues involved in the FCA claims differ from those involved in relator's employment-based claims. Relator's FCA claims concern fraud that defendants allegedly perpetrated on the government, while relator's employment-based claims concern the alleged violation of his own rights during his employment. Resolution of relator's employment-based claims will not narrow the factual and legal issues underlying the FCA claims. While relator brings one of his employment claims under the FCA, “[t]he elements differ for a FCA violation claim and a FCA retaliation claim.” Mendiondo v. Centinela Hosp. Med. Ctr., 521 F.3d 1097, 1103 (9th Cir. 2008). Moreover, a stay would unnecessarily work to delay resolution of relator's FCA claims, which have been pending for more than three years.

Accordingly, the court will refer relator's employment-based claims, Counts Four, Five, and Six, to arbitration and stay proceedings as to these claims only.

IT IS THEREFORE ORDERED that defendants' Motion to Dismiss Relator's Second Amended Complaint (Docket No. 50) be, and the same hereby is, GRANTED IN PART. Count Three of relator's Second Amended Complaint is DISMISSED WITH PREJUDICE. The motion is DENIED in all other respects.

IT IS FURTHER ORDERED that defendants' Motion to Compel Arbitration and Stay Proceedings (Docket No. 50) be, and the same hereby is, GRANTED with respect to Counts Four, Five, and Six of relator's Second Amended Complaint. Proceedings as to Counts One and Two are not stayed.

All Citations

381 F.Supp.3d 1240

Footnotes
In total, relator alleges that AR entered into at least six contracts with the DoD between February 2014 and April 2015 (id. ¶¶ 84-93) and at least nine contracts with NASA between March 2014 and April 2016 (id. ¶¶ 105-114).

Defendants correctly observe that relator’s FCA claims must not only be plausible but pled with particularity under Federal Rule of Civil Procedure 9(b). See Cafasso ex rel. United States v. Gen. Dynamics C4 Sys., Inc., 637 F.3d 1047, 1054–55 (9th Cir. 2011). However, defendants reference Rule 9(b) only to the extent they argue that relator has failed to plead particular facts in support of materiality. (See Mot. to Dismiss at 2-3, 15 & 18.) Therefore, the court assumes, without deciding, that relator has otherwise satisfied the requirements of Rule 9(b).

The court recognizes that “allegations of fraud based on information and belief usually do not satisfy the particularity requirements under rule 9(b).” Moore v. Kayport Package Exp., Inc., 885 F.2d 531, 540 (9th Cir. 1989) (citation omitted). However, as explained elsewhere in this motion, there are other parts of the complaint that allege fraud with sufficient particularity for the purposes of Rule 9(b).

Because relator’s complaint references the documents contained in defendants’ Exhibits Y & Z (Docket Nos. 52-25 & 52-26) in his complaint, the court considers these materials, without converting the motion to dismiss into a motion for summary judgment, under the doctrine of incorporation by reference. See United States v. Ritchie, 342 F.3d 903, 908 (9th Cir. 2003).

Defendants argue for the first time in their reply that these alleged misstatements were not associated with a claim for payment and thus cannot support liability under the FCA. (See Reply in Supp. of Mot. to Dismiss (“Reply”) at 4 (Docket No. 54).) Contrary to defendants’ understanding, the FCA merely requires that the false statement(s) or fraudulent course of conduct cause the government to pay out money due. See Hendow, 461 F.3d at 1173. Under a promissory fraud theory, the relator only needs to allege that a claim was submitted “under a contract” that “was originally obtained through false statements or fraudulent conduct.” See id.; see also United States ex rel. Campie v. Gilead Scis., Inc., 862 F.3d 890, 902 (9th Cir. 2017) (reaffirming Hendow’s test for promissory fraud after Escobar). Here, relator alleges that AR secured its contracts with the government through misrepresentations made to government contracting agents and that the government ultimately paid out on these contracts. (See SAC ¶¶ 59-66, 129-131.)

This promissory fraud theory, supported by these allegations of specific misrepresentations, distinguishes this case from United States ex rel. Mateski v. Raytheon Co., No. 2:06-CV-03614 ODW KSX, 2017 WL 3326452 (C.D. Cal. Aug. 3, 2017), aff’d, 745 F. App’x 49 (9th Cir. 2018). In Mateski, the relator merely alleged general violations of contract provisions that the government designated compliance with as mandatory to support a false certification theory. See id. at *7. Applying Escobar, the district court concluded that “such designations do not automatically make misrepresentations concerning those provisions material.” Id. (citing 136 S. Ct. at 2003).

The court GRANTS defendants’ request that it take judicial notice of these exhibits. Exhibits T through V are publications on government websites and thus properly subject to judicial notice. See, e.g., Daniels-Hall v. Nat’l Educ. Ass’n, 629 F.3d 992, 998-99 (9th Cir. 2010) (finding that it is “appropriate to take judicial notice of [information on government website], as it was made publicly available by government entities [ ], and neither party disputes the authenticity of web sites or the accuracy of the information displayed therein.”). Exhibit S is an official Authorization to Operate signed by NASA officials, so its “accuracy cannot reasonably be questioned.” See Fed. R. Evid. 201(b)(2).

The court expresses no opinion as to what relator will be able to establish at summary judgment or trial.

All remaining Requests for Judicial Notice (Docket No. 52) are DENIED as MOOT.