



PROGRAM MATERIALS

Program #31137

August 10, 2021

Regulating Ransomware: Legal and Insurance Risk Management Guidance and the Collateral Consequences of an Attack

Copyright ©2021 by

- **Michael Kleinman, Esq. - Fried, Frank, Harris, Shriver & Jacobson LLP**
- **Marc Schein, CIC, CLCS - Marsh & McLennan Agency**

**All Rights Reserved.
Licensed to Celesq®, Inc.**

Celesq® AttorneysEd Center
www.celesq.com

5255 North Federal Highway, Suite 100, Boca Raton, FL 33487
Phone 561-241-1919



MARSH & McLENNAN
AGENCY

| FRIED FRANK

Regulating Ransomware

Legal and Insurance Risk Management Guidance and the Collateral Consequences of an Attack

Presenters

Marc Schein

Michael A. Kleinman

August 10, 2021

It's our business
to be there for you in the

**MOMENTS
THAT
MATTER.**

WORLD CLASS. LOCAL TOUCH.



Intro to Ransomware

- Ransomware is a type of malicious software that blocks access to a computer system or data stored therein.
- **WHAT:** Two types of ransomware:
 - Non-encrypting: locking access to system and demanding payment of a ransom to unlock.
 - Encrypting: encrypting files themselves, threatening to destroy or leak documents, and demanding a ransom in exchange for a decryption key.
- In 2020, FBI received **2,474** complaints with adjusted losses of over **\$29.1 million**. Adjusted losses more than **tripled** from 2019 to 2020.¹
- **WHO:** A pattern of coordinated attacks by sophisticated cybercriminal organizations.
 - Evil Corp: Russian-based organization that used ransomware to attack financial institutions **in over 40 countries** and caused **more than \$100 million in theft**.
- Ransomware as a Service – sharing the wealth: business model used by ransomware developers.
 - Clients pay developers to create their own ransomware variants and launch cyber attacks.



Ransomware Payments

- In cryptocurrency (usually bitcoin)
 - Secure
 - Inbound traceability
 - Outbound anonymity



Reasons to Pay Ransom

- Avoid expensive rebuilds
 - SamSam attack against City of Atlanta in March 2018
 - **\$51,000** ransom demand
 - **\$17 million** in network rebuild and other estimated costs
- End business interruption costs from downtime (e.g., interruption to delivery of goods and services)
- Reduce reputational damages
 - Doing everything in your power to reclaim control over your systems and data.
- Perceived lower risks of data exposure
 - Hope that if you pay, “they” will move on to the next target.

OUTAGE ALERT

The City of Atlanta is currently experiencing outages on various customer facing applications, including some that customers may use to pay bills or access court-related information. Our @ATL_AIM team is working diligently with support from Microsoft to resolve this issue. Atlantaga.gov remains accessible. We will post any updates as we receive them. Thank you for your patience.





Reasons Not to Pay Ransom

- No honor among thieves:
 - In Q4 2020, 70% of ransomware attacks involved the threat to leak exfiltrated data.²
 - Double extortion.
- Encouraging further ransomware attacks.
- No guarantee that access to data will be recovered.
- Even adversaries' best intentions may not meet your expectations (e.g., failed decryption, inadvertent deletion of data sets, loss of data integrity (alteration/modification of data)).
- Sanctions from the Office of Foreign Assets Control ("OFAC").

2. Coverware Q4 2020 Ransomware Marketplace report, <https://www.coveware.com/blog/ransomware-marketplace-report-q4-2020>



Office of Foreign Assets Control (“OFAC”)

- Enforcement Agency of the U.S. Treasury Department
 - Primary task is to administer and enforce economic and trade sanctions based on US foreign policy and national security goals against people and places (targeted foreign countries and regimes, terrorists, international narcotics traffickers, those involved in threats to national security, foreign policy or the economy).
- Specially Designated Nationals And Blocked Persons List (“SDN”)
 - Individuals and companies owned or controlled by, or acting for or on behalf of, targeted countries;
 - Individuals, groups, and entities, such as terrorists and narcotics traffickers designated under specific OFAC programs; and/or
 - Assets that are blocked and with which U.S. persons are generally prohibited from dealing.



OFAC Enforcement Powers

- [Economic Sanctions Enforcement Guidelines \(31 CFR part 501, app. A\)](#)
- Select Range of OFAC Responses to Apparent Violations:
 - No Action – insufficient evidence of violation and/or based on “General Factors,” conduct does not warrant administrative response.
 - Violation, No Penalty – no penalty warranted, but may identify compliance policies, practices/procedures deficiencies and identify need for further compliance steps to be taken.
 - Civil Monetary Penalty – violation has occurred and General Factors warrant penalty.
 - Criminal Referral – refer to law enforcement for criminal investigation/prosecution under the International Emergency Economic Powers Act (50 U.S.C. § § 1701—1708) and the Trading With the Enemy Act (50 U.S.C. § § 4301—4341)
- Civil Monetary Penalties of up to the greater of \$311,562 or twice the amount of the underlying transaction.
- Upon Conviction – generally, criminal penalties up to \$1 million, imprisonment for up to 20 years, or both.



General Factors Affecting Administrative Action (31 CFR App. A to Part 501)

- A. Willful or Reckless Violation of Law:
 - 1. Willfulness – decision to take action with knowledge that such action would violate U.S. law?
 - 2. Recklessness – disregard for U.S. sanctions requirements or failure to exercise a minimal degree of caution or care, ignoring warning signs?
 - ***
 - 5. Prior Notice – on notice, or reasonably should have been on notice, that conduct or similar conduct constituted a violation of U.S. law?
- B. Awareness of Conduct at Issue: Generally, the greater a Subject Person's actual knowledge of, or reason to know about, the conduct constituting an apparent violation, the stronger the OFAC enforcement response will be.



General Factors Affecting Administrative Action (cont'd)

- C. Harm to Sanctions Program Objectives: the actual or potential harm to sanctions program objectives caused by the conduct giving rise to the apparent violation:
 - 1. Economic or Other Benefit to the Sanctioned Individual, Entity, or Country: the economic or other benefit conferred or attempted to be conferred to sanctioned individuals, entities, or countries.
 - 2. Implications for U.S. Policy: the effect that the circumstances of the apparent violation had on the integrity of the U.S. sanctions program and the related policy objectives involved.
 - 3. License Eligibility: whether the conduct constituting the apparent violation likely would have been licensed by OFAC under existing licensing policy.
- E. Compliance Program: the existence, nature and adequacy of a risk-based OFAC compliance program at the time of the apparent violation, where relevant.



General Factors Affecting Administrative Action (cont'd)

- F. Remedial Response: corrective action taken in response to the apparent violation, whether new and more effective internal controls and procedures have been adopted to prevent a recurrence. If no prior OFAC compliance program in place at the time of the apparent violation, has one been implemented? If program was in place, have appropriate enhancements been made to prevent recurrence? Have individuals responsible for the apparent violation been given additional training?
- G. Cooperation with OFAC: the nature and extent of cooperation with OFAC, including discretionary consideration of the following:
 - 1. Voluntarily self-disclose?
 - 2. Provide all relevant information to OFAC (whether or not voluntarily self-disclosed)?
 - 3. Research and disclose to OFAC relevant information regarding any other apparent violations caused by the same course of conduct?
 - 4. Provide information voluntarily or in response to an administrative subpoena?
 - 5. Cooperate with, and promptly respond to, all requests for information?



General Factors Affecting Administrative Action (cont'd)

- 6. Enter into a statute of limitations tolling agreement, if requested by OFAC (particularly where apparent violations are not immediately notified to or discovered by OFAC, in particularly complex cases, and in cases in which the Subject Person has requested and received additional time to respond to a request for information)?



EO 13694: Targeting Malicious Cyber-Enabled Activities (cont'd)

- Executive Order 13694 (April 1, 2015): “Blocking the Property of Certain Persons Engaging in **Significant Malicious Cyber-Enabled Activities**”
- Targeting Threat Actors
 - Motivated by “the increasing prevalence and severity of **malicious cyber-enabled activities** originating from, or directed by persons located ... outside the United States” and posing “an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States.”
 - Blocking property and interests in property of any person determined by the Secretary of Treasury, in consultation with the Attorney General and the Secretary of State to be responsible for or complicit in, directly or **indirectly**, engaging in “malicious cyber-enabled” activities originating in whole or substantial part outside of the US that are “reasonably likely to result in, or have materially contributed to, a significant threat to the national security, foreign policy, or economic health or financial stability of the United States” and that have the purpose of:



EO 13694: Targeting Malicious Cyber-Enabled Activities (cont'd)

- Harming/compromising provision of services by computers supporting entities in **critical infrastructure sector**;
- **causing significant disruption to availability of a computer or network of computers; or**
- Causing significant misappropriation of funds or economic resources, trade secrets, personal identifiers or financial information for commercial or competitive advantage or private financial gain.



EO 13694: Targeting Malicious Cyber-Enabled Activities (cont'd)

Application to non-threat actors

- Section 3 makes clear that the prohibitions of EO 13694 apply to “the making of any contribution or **provision of funds**, goods, or services, by, **to**, or for the benefit of **any person** whose property and interests in property are blocked pursuant to this order.”
- OFAC FAQ 445³ (2016): What are your compliance obligations?
 - Don’t engage in trade/transactions with persons on the SDN list or entities owned by them.
 - U.S. persons (including firms that facilitate or engage in online commerce) must ensure they do not engage in unauthorized transactions/dealings with persons on the SDN list or in banned jurisdictions.

Authorizing Treasury to promulgate rules and regulations necessary to carry out the purposes of the order.

3. <https://home.treasury.gov/policy-issues/financial-sanctions/faqs/topic/1546>



Cyber-Related Sanctions Regulations (31 C.F.R. §§578 et seq.)

- The Cyber-Related Sanctions Program is bare bones.
 - Common for “list-based” sanctions programs to offer little interpretative guidance.
- Preliminary Note: “OFAC intends to supplement this part with a more comprehensive set of regulations, which may include additional interpretive and definition guidance, including regarding ‘cyber-enabled’ activities....”
- Much of the program is SDN and blocked property-centric.
- Definitions – No specific definition of significant malicious cyber-enabled activities.
- Regulations provide little interpretative guidance on the broad language of the Executive Order.
- Possibility to obtain license:
 - General License (§ 578.306(b)) – license or authorization identified by OFAC.
 - Specific License (§ 578.306(c)) – license or authorization specifically obtained.



2017 OFAC Guidance on Cyber Sanctions

“Sanctions Against Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities” (2017)

- Summary of existing authorities and potential penalties.
- “OFAC intends to supplement the Regulations with a more comprehensive set of regulations, which may include additional interpretative and definitional guidance and additional general licenses and statements of licensing policy.”
 - THEY DID NOT

Further Explanation of Licenses

- General Licenses – “types or categories of activities and transactions that would otherwise be prohibited with respect to cyber-related sanctions.”
 - Ex: Section 578.506 of the Regulations allows certain legal services to be provided to SDNs.
 - Ex: General License No. 1 – authorizes certain transactions with Russia’s Federal Security Service related to importation, distribution or use of certain information technology products.
- Specific Licenses – authorization of otherwise banned transactions will be considered on a case-by-case basis, but does not provide any criteria for how to make a decision.



The October 2020 Advisory

“Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments”

- Advisory, means “explanatory only;” does not have the “force of law.”

Warning to Advisors: “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 may also risk violating OFAC regulations.***”

Legal Reminders

- Strict Civil Liability: a US person may be held civilly liable even if it did not know or have reason to know it was engaging in a transaction with a prohibited person.
- Power to Refer for Criminal Liability: Under IEEPA and TWEA.

Sanctions Nexus: U.S. persons are prohibited from engaging in transactions, directly or indirectly, with individuals or entities on the SDN list, or any individuals or entities with a “**sanctions nexus**” to SDNs.

- **No definition of “sanctions nexus”**

Two Certainties in the October 2020 Advisory

OFAC Licensing Policy

License applications involving ransomware payments are reviewed on a case-by-case basis with a **presumption of denial**.

- Whereas prior guidance left open the possibility of obtaining a specific license, the Advisory makes clear that the chance of getting a license approved for a ransomware payment is extremely remote.
 - Practical Difficulties: Time to get a specific license approved is weeks, if not months.

Cooperation and Communication is a Significant Mitigating Factor

Self-initiated, timely, and complete report of a ransomware attack to law enforcement will be considered as a **significant mitigating factor** in determining an appropriate enforcement outcome if the situation is later determined to have a sanctions nexus.

Full and timely cooperation with law enforcement both during and after a ransomware attack will be a **significant mitigating factor** when evaluating a possible enforcement outcome.



Sanctions Nexus? Unanswered Questions

1. “This advisory describes these sanctions risks and provides information for contacting relevant U.S. government agencies, including OFAC, if there is a reason to believe the cyber actor demanding ransomware payment may be sanctioned or otherwise have a sanctions nexus.”
 - *If a payment is not sanctioned (i.e., paid to a banned person, account or jurisdiction), what is the additional sanctions nexus?*
2. “Ransomware Payments with a Sanctions Nexus Threaten U.S. National Security Interests.”
 - *What is a payment with a sanctions nexus?*
3. “Under OFAC’s Enforcement Guidelines, OFAC will also consider a company’s self-initiated, timely, and complete report of a ransomware attack to law enforcement to be a significant mitigating factor in determining an appropriate enforcement outcome if the situation is later determined to have a sanctions nexus.”
 - *What is a company’s or facilitator’s obligation to continue to monitor for a “later determined” sanctions nexus?*
4. “OFAC encourages victims and those involved with addressing ransomware attacks to contact OFAC immediately if they believe a request for a ransomware payment may involve a sanctions nexus.”
 - *When? And ... what is a sanctions nexus?*



Difficulties with Discovering a Sanctions Nexus

- SDN list includes at least 161 known cyber threat actors as of August 9, 2021.
- Infrastructure and protection of ransomware threat actors is obfuscated and to a large extent protected at the federal level in specific geographic regions including Russia.
- Most threat actors use one or more digital currency wallets and exchanges for each victim, and often split payments after initial receipt of cryptocurrency using mixing services (e.g. tumblers) to increase the anonymity of their transactions, making tracing extremely difficult for federal law enforcement, if not impossible for civilians.
- Recent proliferation of Ransomware-as-a-Service (“RaaS”) – buying or leasing ransomware variants to launch an attack – further masks identity of the threat actors and other payees.
- Most RaaS groups partner with access brokers who initially compromise the victim network then sell access to the ransomware threat actors who deploy ransomware. This makes attribution during the OFAC process difficult.

Advisory Reminder on Risk-Based Compliance Obligation

The Advisory encourages companies to implement a Sanctions Compliance Program (“SCP”) following OFAC’s Risk-based Compliance Commitment Framework to mitigate exposure to sanctions-related violations:

1. **Management Commitment** – senior management should review and approve the SCP, ensure direct reporting line from compliance unit, ensure unit has resources (human capital, expertise, IT).
2. **Risk Assessment** – “holistic” 360 degree review of organization’s “touchpoints to the outside world” that evolves with the organization, including scrutinizing customers and relationships.
3. **Internal Controls** – implementation of (i) policies and procedures that can “adjust rapidly” to changes in SDN list and updated/amended/new sanctions programs implemented by OFAC; (ii) recordkeeping controls; and (iii) process to ensure external parties performing SCP on behalf of organization do so properly.
4. **Testing and Auditing** – identify weaknesses and deficiencies, marshal necessary resources to enhance SCP, and remediate any gaps.
5. **Training** – train all employees and personnel at least annually, communicate compliance responsibilities for each individual.

Implementing the Ransomware Advisory: A Response Checklist

1. Get the facilitators on board: retain and consult counsel, forensic investigators, negotiators and insurance professionals.
 - Lawyers familiar with dealing with OFAC.
 - Forensic Investigators, Negotiators and Insurance Professionals to *try to* identify threat actors based on Indicators of Compromise (IOCs) and Tactics, Techniques, and Procedures (TTPs).
2. If Paying, document analysis and determination.
 - Document what you did and what you looked at to rule out a possible sanctions nexus.
 - Document identifying details and accounts for actor paid.
3. Determine whether to notify law enforcement and when.
4. If **Paid**, continue post-hoc screening of SDNs once payment has been made.
 - To account for post hoc “sanctions nexus” – ensure that SCP includes record keeping to document digital currency wallet accounts and other identifying features. Then set alerts for hits based on additions of new SDNs that might match individuals, organizations, and wallets paid.

Exxon Mobil Corp. v. Mnuchin⁴: Background

On March 16, 2014, President Obama issued Executive Order 13361 to impose sanctions on Ukraine and Russia-related parties.

- Section 1: "blocked" property that is "within the possession or control" of any United States individual or entity cannot "be transferred, paid, exported, withdrawn, or otherwise dealt in" by SDNs.
- Section 4: the prohibitions of Section 1 "include . . . the **receipt of any contribution or provision of ... services.**"

In April 2014, the Treasury designated Igor Sechin as a SDN. His company, Rosneft, a Russian petroleum company, was not designated as an SDN.

On May 14, 2014, OFAC issued the Ukraine-related sanctions regulations that prohibited all transactions under the Executive Order 13361.

On May 23, 2014, Exxon entered eight contracts with Rosneft, each signed by Sechin.

On August 13, 2014, OFAC published FAQ 400 and clarified that "OFAC sanctions generally prohibit transactions involving, directly or indirectly, a blocked person . . . even if the blocked person is acting on behalf of a non-blocked entity."

In June 2015, OFAC imposed a civil penalty of \$2,000,000 on Exxon, on the ground that the transactions with Rosneft violated Section 4 of Executive Order 13661, which **prohibits the receipt of services from a blocked individual.**

Exxon Mobil Corp. v. Mnuchin: Fifth Amendment Defense

Exxon challenged OFAC's penalty asserting OFAC failed to provide fair notice of its interpretation of the Regulations in violation of the Due Process Clause of the Fifth Amendment.

The District Court agreed.

- Legal Standard:
 - Under the Due Process Clause of the Fifth Amendment, laws that regulate individuals or entities "must give fair notice of conduct that is forbidden or required."
 - In the administrative law context, "fair notice requires the agency to have 'state[d] with **ascertainable certainty** what is meant by the standards [it] has promulgated.'"
- Analysis:
 - The text of the Regulations provides no fair notice of OFAC's interpretation of the language of EO 13661 because it **fails to address what constitutes a "receipt" of services**.
 - "Exxon's alleged violation is based on the receipt of a service, and the service was Sechin's act of signing. When does an entity 'take,' 'come into possession,' or 'get' a service? On this point, the Regulations are silent."
 - OFAC issued an FAQ explicitly prohibiting Exxon's conduct **after** Exxon's alleged violations. This timing supports the conclusion that the Regulations' text fails to provide ascertainable certainty.



Defense against the Imposition of a “Sanction Nexus”

Exxon can well serve as a roadmap for a defense to sanctions enforcement against a ransomware victim and its advisors.

The vague description of “sanctions nexus” does not clear the ultimate hurdle of “ascertainable certainty” required by the Fifth Amendment.

- The Executive Orders, the FAQs, the 2020 Guidance, and other OFAC public statements have not given any definition on the term.
- The term “sanctions nexus” is *only* contained in the Advisory, and OFAC purports to define fully the term in a matter of a few sentences in the Advisory containing non-exhaustive hypotheticals.
- A court applying *Exxon* to the “sanctions nexus” language might likewise hold that the Regulations are vague, overly broad, and that the OFAC guidance “fails to delineate their boundaries.”



NOTE ON FinCEN

The 2020 OFAC Advisory stated that 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.

- References sister advisory released the same day: “Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments,” which provides guidance on anti-money-laundering obligations related to financial institutions in the context of ransomware payments.
- June 30, 2021 – FinCEN’s national anti-money-laundering priorities includes cybercrime.
 - Promises regulations clarifying how financial institutions should incorporate priorities into their existing AML compliance programs.

Insurance Circular Letter No. 2 (2021): Cyber Insurance Risk Framework: A Warning to Insurers from NY DFS

February 4, 2021 – Citing 2020 OFAC Advisory, New York State Department of Financial Services joins law enforcement in recommending against ransom payments.

Raising concerns that insurers are bearing increasing cyber risk yet are unable to accurately measure the risk.

Urging insurers to develop a rigorous and data driven approach to cyber risk:

- 1. Establish a formal cyber insurance risk strategy
- 2. Manage and eliminate exposure to silent cyber insurance risk
- 3. Evaluate systemic risk
- 4. Rigorously measure insured risk
- 5. Educate insureds and insurance producers
- 6. Obtain cybersecurity expertise
- 7. Require notice to law enforcement



Ransomware Attacks Targeting Insurance Companies

AXA

- Ransomware attacks after AXA announced it no longer insured ransomware payments in France
- Hitting IT operations in Thailand, Malaysia, Hong Kong, and the Philippines
- Personal data and medical records stolen

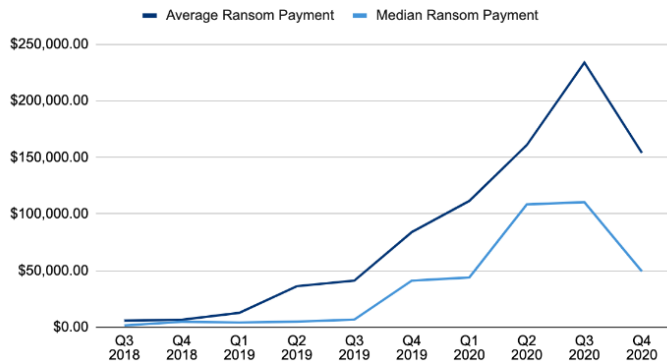
CNA Financial

- Malware encrypted data on over 15,000 machines on CNA's company network
- Employees were locked out of the company's systems and confidential data was stolen
- Reportedly paid \$40 million

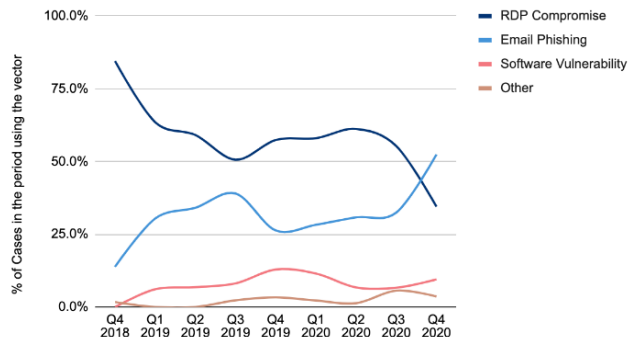
4th Quarter 2020 Coveware Report

- Average Ransom Payment decreased 34% in Q4 '20 from \$233,817 to \$154,108*
- 70% of the Ransomware Cases use Data Exfiltration as a Tactic (Up from half in Q3 2020)
- Average Employee Size of Company impacted = 234 (+39% from Q3 2020)
- Average Days of Downtime = 21 Days (+11% from Q3 2020)

Ransom Payments By Quarter



Ransomware Attack Vectors











2021 Cyber Insurance Market Conditions Tighten

Cyber market conditions continue to deteriorate:

- Appetite changes and increased requirements are the new normal in 2021, there is little steady-ground as carriers make changes on a monthly, if not weekly, basis.
- The **very best risks** are seeing increases of +25-50%; Marsh reports that Cyber premiums are trending up, on average, 56% as of Q2 2021 (total program).
- Healthcare risks saw a 67.8% increase on their cyber placements as of Q2 2021.
- Manufacturing risk saw a 67.6% increase on their cyber placements as of Q2 2021.
- 83% of power and utilities companies saw a increase on their cyber insurance as of Q2 2021.
- 92% of Marsh USA clients received an increase on their cyber insurance as of Q2 2021.
- Increases of 100% – 300% are not unusual.
- \$10M limits are difficult to come by and are no longer available on the vast majority new business.
- Dramatic changes in the reinsurance marketplace.

Carrier change of focus from **Respond and Recover** to **Educate and Prevent**

Cyber Insurance Market Snapshot

Pricing & Terms		Claims		Underwriting	
Rates	Limits / Coverage	Frequency	Severity	Information Needs	Carrier Flexibility
 <p>Average premium increase in</p> <ul style="list-style-type: none"> Oct 2020: 11% Nov 2020: 17% Dec 2020: 26% Jan 2021: 29% Feb 2021: 32% Mar 2021: 39% April 2021: 40% 	 <p>Many carriers are reducing capacity exposed. Some carriers are scaling back ransomware-related coverages (or not offering coverage at all) for clients that don't have adequate controls.</p>	 <p>Ransomware is more accessible for bad actors. Short tail nature of losses is changing insurer profitability weekly.</p>	 <p>Ransom payments in the millions. Business interruption and data recovery loss. Solar Winds & MS Exchange attacks have increased carrier uncertainty around systemic nature of cyber risk.</p>	 <p>Full application & responses to ransomware Q's. Underwriters will inquire about usage of Solar Winds services and Microsoft Exchange servers.</p>	 <p>Ransomware responses required prior to quoting. Third party scans may lead to remediation requests. Minimum controls are required to obtain a quote.</p>

Future Expectations

Anticipate increases to accelerate, likely **50% or greater** in Q2 and beyond; terms dependent on risk profile & controls.

Future Expectations

Ransomware attacks will continue to increase in sophistication; systemic risks concerns; privacy risk concerns.

Future Expectations

Underwriters will demand additional information to assess risk and may require certain cyber controls to quote.



Favors Buyer



Neutral



Favors Insurers



Fitch Ratings: U.S. Cyber Insurance Market Update

Fitch estimates industry direct written premium for cyber coverage in standalone and package policies increased to approximately \$2.7 billion.

Written premiums for standalone cyber coverage increased by 29% for the year, reflecting growing demand for specific cyber protection.

The average paid loss for a closed standalone cyber claim jumped to \$358,000 in 2020 from \$145,000 in 2019, according to a recent report by Fitch Ratings.

The direct loss ratio for standalone cyber rose sharply in 2020 to 73%, the highest level recorded in the six years that separate cyber data were included in financial reporting.

Fitch Ratings: U.S. Cyber Insurance Market Update (cont'd)

- Demand for coverage is driven by the need for risk management expertise and insurance protection by firms of all sizes due to incidence of network intrusions, data theft and ransomware incidents that have increased substantially in the last two years.
- Underwriters, especially those new to the coverage area, are challenged by limited historical claims and underwriting data.
- Insurers will need additional changes in risk selection and policy terms, including coverage exclusions and sub-limits, if they are to realize a significant turnaround in underwriting performance.
- **Any reduction in cyber incidents and losses will ultimately be tied to organizations implementing more effective risk prevention and event remediation measures.**

Cyber Insurance Renewal Expectations for Clients

- **Expectations:** Set appropriate expectations with your leadership team/Broker.
- **Premium Rates:** are going up on most accounts.
- **Cybersecurity Controls:** MOST risks will be heavily underwritten for cybersecurity controls & procedures.
 - Understand the carrier-specific dynamics below, and that they change!
 - Minimum security controls that are strongly recommended:
 - MFA, Disabled RDP for all External Access, Encryption & Segmentation, Tested Backups, Endpoint Detection and Response, Firewalls, etc.
 - Entities that do not have these controls in place are seeing drastic increases in pricing/deductibles, reduction in coverage or non-renewal.
- **Applications:** gather plenty of information at renewal – suggestions
 - Main form (in lieu of renewal) application.
 - Carrier's ransomware supplemental form (if applicable).



Cyber Insurance Renewal Expectations for Clients (cont'd)

- **No Guarantees:** Renewal terms from incumbents are not guaranteed, you may want to assume that renewal terms *will not* be offered, or will require replacement due to extremely unfavorable terms/conditions.
- **Give Yourself Time:** Be *at least* 90 days ahead of cyber renewal deadlines.



Cyber Carrier and Coverage Updates

Some carriers exiting the marketplace all together.

Several carriers have implemented **Coinurance** or **Sublimited** coverage on Extortion losses (i.e., ransomware) or

- May apply to all of the claim not just ransomware.
- **Coinurance**: the amount an insured must pay against a claim after the deductible is satisfied.
- **Sublimit**: a limitation in an insurance policy on the amount of coverage available to cover a specific type of loss.

[Nearly all] carriers are requiring more underwriting information:

- Supplemental applications (MFA Supplemental)
- Extrusive technology scans of insured's networks
- Strongly recommending Tech Solutions be deployed before providing terms or competitive terms are offered
- [Requiring] employee training
- [Requiring] written policy and procedures
- **Strong focus on pre-breach services**



2021 Changes in Underwriting

Name of Applicant:

Address:

City:

State:

Zip:

Telephone:

Date Established:

State of Incorporation:

Website:

Revenues:

Type of Private Information	Estimated Number of Records
Personal Identifiable Information (PII) - (i.e. - Social Security, Driver's License, Customer Information)	
Personal Healthcare Information (PHI) - (i.e. - Medical Records, Health Insurance Account Information)	
Financial Information - (i.e. - Credit Cards, Bank Account Information, Money/Securities Information)	
Third Party Corporate Information - (i.e. -Non- Disclosure Contract)	



2021 Changes in Underwriting (cont'd)

SECURITY, PRIVACY & MEDIA CONTROLS – Do You Have the Following Controls in Place?

- Firewalls
- Anti-Virus
- Encryption – At Rest, In-Transit and/or Mobile Devices
- Intrusion Detection/Prevention or End-Point Detection/Response
- Vulnerability Scanning/Patching
- Is user access to critical or sensitive repositories audited periodically?
- Is Multifactor Authentication in use?
- Does the organization Backup Electronic Data?
 - Are backups encrypted?
 - Are the credentials used to access backups unique (i.e., not reused for another account)?
 - Has the recovery of critical systems from backups been documented?
 - ♦ Has the recovery of critical systems from backups been tested?
 - ♦ What is the time to restoration?



2021 Changes in Underwriting (cont'd)

- Are backups Physically or Digitally Segregated from your organization's network?
- How frequently is data backed up?
- Who is responsible for managing backups?
- BCP, DR & IRP – Business Continuity, Disaster Recovery and/or Incident Response Plans. Do you have the plans & have they been tested?
- Written Information Security Policy (WISP) and/or Privacy Policy
- Vendor Risk Management Protocols – Cyber Risk Controls and Contracts (Liabilities, Indemnification, etc.)
- Regulatory Compliance – GDPR, CCPA, HIPAA, BIPA, etc.
- Compliance with Payment Card Industry Data Security Standards (PCI-DSS)
- Employee-training program relating to Cyber Risk
- Content Review Process – Review Content/Material being disseminated prior to release
- Attain proper licensing for Content/Material
- Procedures in place to remove controversial Content/Material



Carrier Concerns based on Loss Data

- **Key Questions:**

- Can you recover your critical systems and data in 10 days?
- Off-site (cloud) back-ups less than a month old?
- Multifactor authentication (remote access, remote email access, privileged accounts, critical data/systems)?



2021 Changes: New Exclusions

- Removing all **Non-IT Service Providers** Business Interruption (BI) coverage on renewals
- **Waiting period** going to 18 hours for BI; 24 hours for contingent BI. Additionally, **50% limits-reducing co-insurance** is applied to all contingent BI claims.
- **Solar Winds & MS Exchange exclusions**
- **Loss of Technical Support exclusion**
 - *A significant reduction in coverage.* Could preclude coverage for Insureds when a vulnerability is exploited in any software or hardware that has reached end-of-life, end-of-support, or where the vendor has withdrawn or no longer supports such program or device. Further, we believe this exclusion could preclude coverage in whole or in part, instances where your outsourced service provider(s) may utilize end-of-life or end-of-support software or hardware, even if you had no knowledge of the vendor using such software or hardware.



Recovering Ransom Payments

Colonial Pipeline Co. Cyber Attack

- Cybercriminal group DarkSide attacked the oil pipeline system on May 7, 2021.
- Company paid 75 bitcoin (about \$4.3 million) within several hours after the attack.

Federal Government recovered 63.7 bitcoins (about \$2.3 million).

- Tracing bitcoin addresses (analogous to bank account numbers; they are virtual locations to which bitcoin are sent and received).
- Using blockchain explorers (online tools that operate as a blockchain search engine that allows users to search for and review transactional data).
- FBI obtained the private key (a cryptographic equivalent of a password needed to access the bitcoin address), but **unclear how**.
- DarkSide shut down its operation on May 17, claiming the U.S. law enforcement agency was behind the disruption.

Questions/Comments?



MARSH & McLENNAN
AGENCY

MarshMMA.com

This document is not intended to be taken as advice regarding any individual situation and should not be relied upon as such. Marsh & McLennan Agency, LLC shall have no obligation to update this publication and shall have no liability to you or any other party arising out of this publication or any matter contained herein. Any statements concerning actuarial, tax, accounting or legal matters are based solely on our experience as consultants and are not to be relied upon as actuarial, accounting, tax or legal advice, for which you should consult your own professional advisors. Any modeling analytics or projections are subject to inherent uncertainty and the analysis could be materially affective if any underlying assumptions, conditions, information or factors are inaccurate or incomplete or should change. Copyright © 2021 Marsh & McLennan Insurance Agency LLC. All rights reserved.

Regulating Ransomware: Legal and Insurance Risk Management Guidance and the Collateral Consequences of an Attack

August 10, 2021

Supplemental Materials

Michael A. Kleinman and Marc Schein

2019 Internet Crime Report



2019 INTERNET CRIME REPORT

TABLE OF CONTENTS

Introduction	3
About the Internet Crime Complaint Center	4
IC3 History	5
The IC3 Role in Combating Cyber Crime	6
IC3 Core Functions	7
Supporting Law Enforcement	8
IC3 Database Remote Access	8
Hot Topics for 2019	9
Business Email Compromise (BEC)	9
IC3 Recovery Asset Team	10
RAT Successes	11
Elder Fraud	12
Tech Support Fraud	13
Ransomware	14
2019 Victims by Age Group	16
2019 - Top 20 International Countries by Victim	17
2019 - Top 10 States by Number of Victims	18
2019 - Top 10 States by Victim Loss	18
2019 Crime Types	19
2019 Overall State Statistics	21
Appendix A: Crime Type Definitions	25
Appendix B: Additional information about IC3 Data	28

INTRODUCTION

Dear Reader,

The FBI is the lead federal agency for investigating malicious cyber activity by criminals, nation-state adversaries, and terrorists. To fulfill this mission, the FBI often develops resources to enhance operations and collaboration. One such resource is the FBI's Internet Crime Complaint Center (IC3) which provides the public with a trustworthy and convenient mechanism for reporting information concerning suspected Internet-facilitated criminal activity. At the end of every year, the IC3 collates information collected into an annual report.

This year's Internet Crime Report highlights the IC3's efforts to monitor trending scams such as Business Email Compromise (BEC), Ransomware, Elder Fraud, and Tech Support Fraud. As the report indicates, in 2019, IC3 received a total of 467,361 complaints with reported losses exceeding \$3.5 billion. The most prevalent crime types reported were Phishing/Vishing/Smishing/Pharming, Non-Payment/Non-Delivery, Extortion, and Personal Data Breach. The top three crime types with the highest reported losses were BEC, Confidence/Romance Fraud, and Spoofing. More details on each of these scams can be found in this report.

Of note, the IC3's Recovery Asset Team (RAT), which assists in recovering funds for victims of BEC schemes, celebrated its first full year of operation. During its inaugural year, the team assisted in the recovery of over \$300 million lost through on-line scams, boasting a 79% return rate of reported losses. We're also pleased to announce the creation of a Recovery and Investigative Development (RaID) Team which will assist financial and law enforcement investigators in dismantling money mule organizations.

Information reported to the IC3 helps the FBI gain a better understanding of cyber adversaries and the motives behind their activities. Therefore, we encourage everyone to use IC3 and reach out to their local field office to report malicious activity. Cyber is the ultimate team sport. Working together we hope to create a safer, more secure cyber landscape ensuring confidence as we traverse through a digitally-connected world.

We hope this report provides you with information of value as we work together to protect our nation against cyber threats.



Matt Gorham
Assistant Director
Cyber Division
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.

The IC3 Recovery and Investigative Development (RaID) Team was created in 2019. Its goal is to partner with financial and law enforcement investigators in an effort to dismantle money mule organizations. RaID comprises two teams: the Recovery Asset Team (RAT) and the Money Mule Team (MMT). While the RAT is primarily focused on financial recovery, the MMT performs detailed analysis and research on previously unknown targets in an effort to develop new investigations. The teams work together under the RaID umbrella to leverage resources from cyber security experts and financial and law enforcement partners to help address the ever-changing and growing problem of cyber-enabled fraud.

RaID enhances investigations by monitoring new activity and notifying law enforcement of time sensitive situations. The team often plays a significant role in uncovering additional victims and criminals involved in fraudulent activity. RaID works as a liaison between financial and law enforcement investigators to facilitate information sharing necessary to support open case work and assist in any required legal process to stop the flow of fraudulent funds.

RaID has partnered with FBI Field Offices to develop an investigative matrix to triage complaint information provided by IC3 victims. The matrix allows analysts and agents to quickly identify potential targets from the hundreds of IC3 complaints received on a daily basis, and to gain a more complete view of the cyber-enabled fraud threat landscape.

These innovative techniques are leading to successful results, even in investigations that have spanned multiple years. For example, the IC3 provided FBI San Francisco with complaints over three years regarding subjects in one of its cases. The complaints reported incidents of SIM SWAPPING, social engineering, online account takeovers, cryptocurrency theft, online threats, extortion, celebrity account hacking, SWATing and Doxxing. San Francisco ultimately arrested three individuals in connection to these complaints, the most recent being the arrest of a SIM SWAPPING group leader which led to the seizures of over \$18 million, five vehicles, a \$900,000 home, and hundreds of thousands of dollars in jewelry. The SIM SWAPPING scheme had targeted hundreds of victims, compromised hundreds of cryptocurrency accounts, and caused approximately \$40 million in losses.

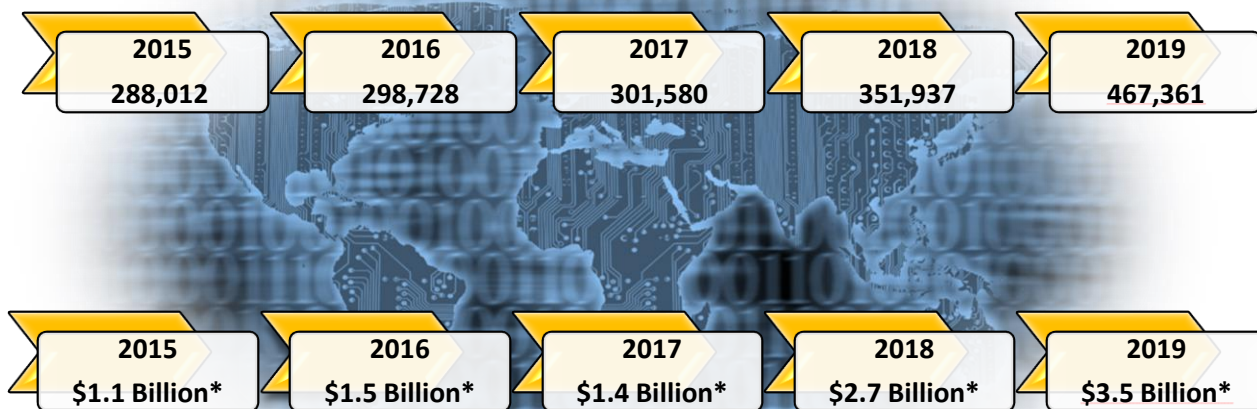
IC3 HISTORY

In May 2000, the IC3 was established as a center to receive complaints of Internet crime. A total of 4,883,231 complaints have been reported to the IC3 since its inception. Over the last five years, the IC3 has received an average of 340,000 complaints per year. These complaints address a wide array of Internet scams affecting victims across the globe.¹

IC3 Complaint Statistics

Last Five Years

1,707,618 TOTAL COMPLAINTS

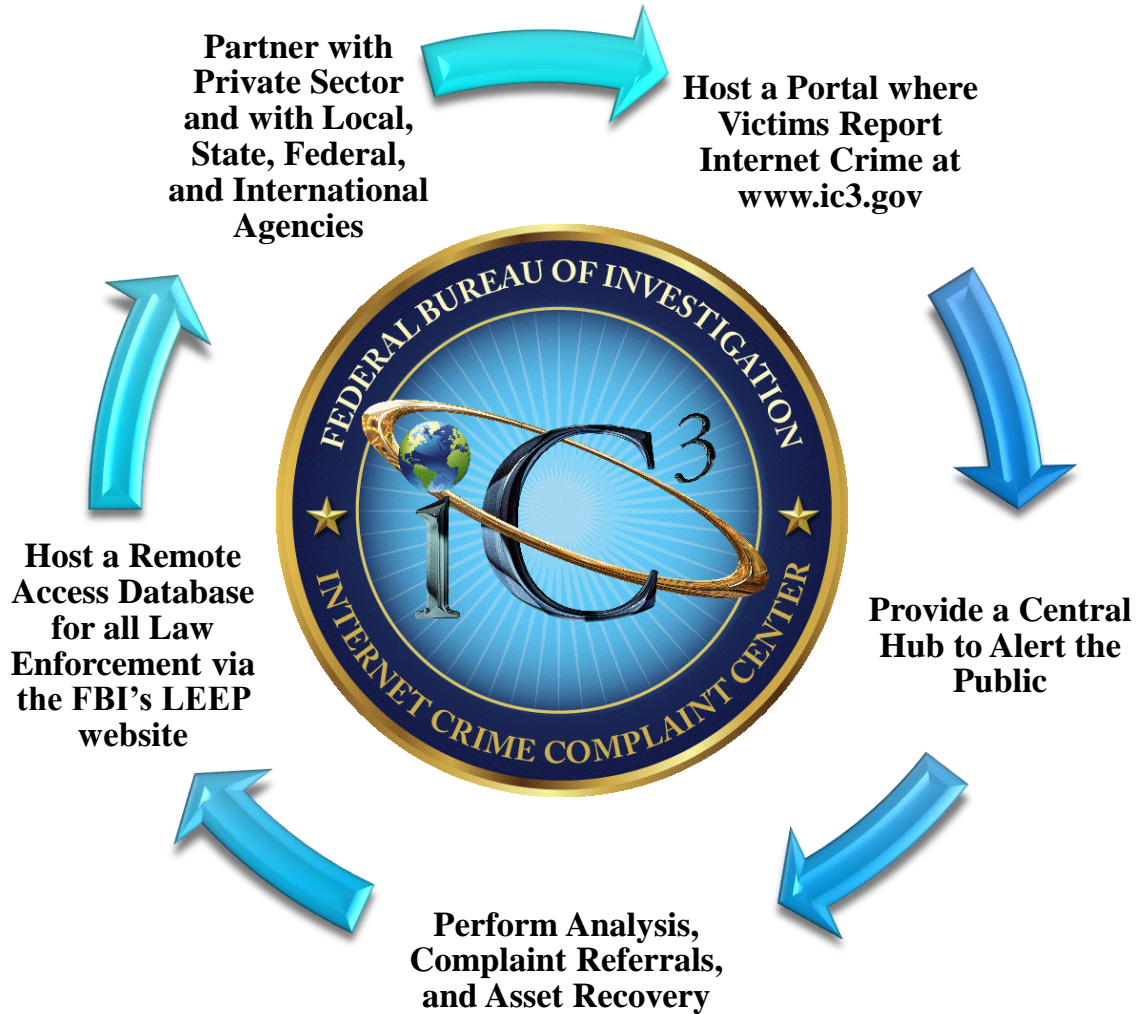


\$10.2 Billion TOTAL LOSSES*

(Rounded to the nearest million)

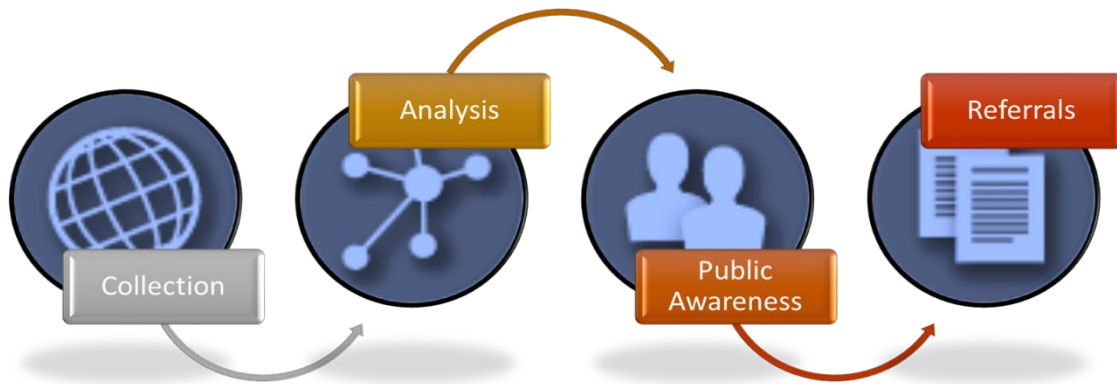
¹ Accessibility description: Image includes yearly and aggregate data for complaints and losses over the years 2015 to 2019. Over that time period, IC3 received a total of 1,707,618 complaints, reporting a loss of \$10.2 billion.

WHAT WE DO



² 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; increase victim reporting via outreach; host a remote access database for all law enforcement via the FBI's LEEP website.

IC3 CORE FUNCTIONS



IC3 Core Functions³

COLLECTION	ANALYSIS	PUBLIC AWARENESS	REFERRALS
<p>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 www.ic3.gov. 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.</p>	<p>The IC3 reviews and analyzes data submitted through its website to identify emerging threats and new trends.</p>	<p>Public service announcements, scam alerts, and other publications outlining specific scams are posted to the www.ic3.gov 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.</p>	<p>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.</p>

³ 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.

SUPPORTING LAW ENFORCEMENT

IC3 DATABASE REMOTE ACCESS

All sworn law enforcement can remotely access and search the IC3 database through the FBI's Law Enforcement Enterprise Portal (LEEP).

LEEP is a gateway providing law enforcement agencies, intelligence groups, and criminal justice entities access to beneficial resources all in one centralized location. These resources can be used to strengthen case development for investigators and enhance information sharing between agencies. This web-based access additionally provides users the ability to identify and aggregate victims and losses within a jurisdiction.



The IC3 has expanded the remote search capabilities of the IC3 database by allowing users to gather IC3 complaint statistics. Users now have the ability to run city, state, county, and country reports, as well as sort by crime type, age, and transactional information. The user can also run overall crime type reports and sort by city, state, and country. The report results can be returned in a PDF or exported to Excel. This search capability allows users to better understand the scope of cyber-crime in their area of jurisdiction and enhance cases.

The IC3 routinely provides training to law enforcement regarding the IC3 database and remote query capabilities. Throughout 2019, the IC3 provided three separate training sessions to state and local law enforcement personnel in Providence, Rhode Island; Grand Rapids, Michigan; and Orlando, Florida, which improved their understanding of FBI information available to law enforcement via LEEP.

HOT TOPICS FOR 2019

BUSINESS EMAIL COMPROMISE (BEC)



In 2019, the IC3 received 23,775 Business Email Compromise (BEC) / Email Account Compromise (EAC) complaints with adjusted losses of over \$1.7 billion. BEC/EAC is a sophisticated scam targeting both businesses and individuals performing a transfer of funds. The scam is frequently carried out when a subject compromises legitimate business e-mail accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds.

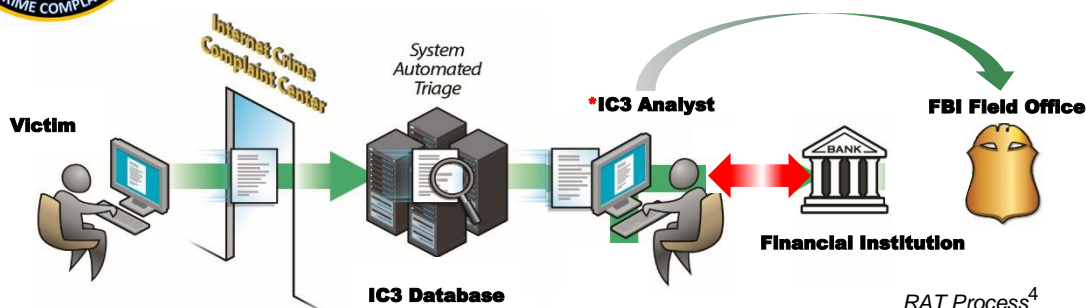
BEC/EAC is constantly evolving as scammers become more sophisticated. In 2013, BEC/EAC scams routinely began with the hacking or spoofing of the email accounts of chief executive officers or chief financial officers, and fraudulent emails were sent requesting wire payments be sent to fraudulent locations. 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 2019, the IC3 observed an increase in the number of BEC/EAC complaints related to the diversion of payroll funds. In this type of scheme, a company's human resources or payroll department receives an email appearing to be from an employee requesting to update their direct deposit information for the current pay period. The new direct deposit information generally routes to a pre-paid card account.

IC3 RECOVERY ASSET TEAM



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



*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).

Recovery 2019:

Incidents: 1,307

Losses: \$384,237,651

Recovery: \$304,930,696

Recovery Rate: 79%

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

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 as well as 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 (real estate, pre-paid cards, W-2, etc.).
- Never make any payment changes without verifying with the intended recipient; verify email addresses are accurate when checking mail on a cell phone or other mobile device.

⁴ 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.

Dallas

In December 2019, the Dallas Field Office reached out to RAT for assistance on a transfer for a \$190,000 BEC incident where the victim wired funds on two separate occasions for invoice payments. The IC3 RAT's quick action, in conjunction with the alliance built with key financial partners, led to the successful recovery of funds. This collaboration between IC3 RAT and their financial partners resulted in the exchange of key information that allowed the IC3 RAT to work in conjunction with the FBI field office to refer the case to local law enforcement. As a result, federal and local law enforcement worked together to ultimately pursue the case, which led to successful prosecution of the perpetrator.

Los Angeles

In November 2019, the IC3 RAT was asked by the Los Angeles Field Office to provide an analytical report that concentrated on elderly victims who fell victim to a variety of scams, including BEC and Romance scams, resulting in the victims transferring funds to possible money mules located in the Los Angeles area of responsibility. The IC3 RAT provided an analytical report that consisted of 19 IC3 complaints and a total loss of over \$866,000. As a result of the research and analysis done by the IC3 RAT, the Los Angeles Field Office was able to conduct multiple interviews and disseminate cease and desist letters to the money mules identified.

Fort Lauderdale

In February 2019, the IC3 RAT received a complaint involving a BEC incident for \$138,000, where the victim received a spoofed email and wired funds to a fraudulent bank account in Florida. The RAT took quick action and worked with key financial partners to freeze the funds. When the perpetrator attempted to withdraw funds, the RAT's collaboration with financial partners enabled the bank employee to request the perpetrator provide documents to support the receipt of the wire. When the account holder was unable to provide legitimate documentation, the bank alerted local law enforcement and as a result, the account holder was arrested by the Fort Lauderdale Police Department.

ELDER FRAUD

The Elder Abuse Prevention and Prosecution Act was signed into law in October 2017 to prevent elder abuse and exploitation and improve the justice system's response to victims in elder abuse and exploitation cases. As a response to the increasing prevalence of crimes against the elderly, especially Elder Fraud, 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 2019, the IC3 released PSAs to educate the public about Romance Fraud, common Elder Fraud schemes, and money mule activity. The FBI has held hundreds of outreach events in order to educate the public about Elder Fraud.

The Department of Justice Consumer Protection Branch (DOJ-CPB) and the FBI have also partnered to pursue fraudsters and facilitators of schemes who target the elderly. In March 2019, the FBI and other federal law enforcement partners undertook an Elder Fraud and Tech Support Fraud sweep, targeting over 260 defendants who had allegedly defrauded over 2 million U.S. victims of more than \$750 million. DOJ-CPB and the FBI also target money mules who serve as the witting or unwitting facilitators of laundering proceeds from Elder Fraud schemes.

In 2019, the IC3 received 68,013 complaints from victims over the age of 60 with adjusted losses in excess of \$835 million. Age is not a required reporting field. These statistics reflect only those 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>.

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 in an effort to defraud unwitting individuals. Criminals may pose as support or service representatives offering to resolve such issues as a compromised e-mail or bank account, a virus on a computer, or a software license renewal. Some recent complaints involve criminals posing as customer support for well-known travel industry companies, financial institutions, or virtual currency exchanges.

In 2019, the IC3 received 13,633 complaints related to Tech Support Fraud from victims in 48 countries. The losses amounted to over \$54 million, which represents a 40 percent increase in losses from 2018. The majority of victims reported to be over 60 years of age.

Additional information, explanations, and suggestions for protection regarding Tech Support Fraud is available in a recently published 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.

Charlotte

A North Carolina man pleaded guilty to conspiracy to access a protected computer, for his role in an international tech support scam that defrauded hundreds of victims, including seniors, of more than \$3 million. The subject was part of a conspiracy that carried out the scam by placing fake pop-up ads on victims' computers to convince them they had a serious computer problem, and to induce them to pay for purported "technical support" services to resolve the issue. The IC3 provided ongoing assistance to the Charlotte Field Office and the prosecuting attorneys in this case.

Philadelphia

A Pennsylvania man pleaded guilty to wire fraud and was sentenced to 15 months imprisonment to be followed by two years of supervised release. The subject admitted to perpetrating a computer-based fraud scheme that targeted victims across the United States. As part of the scheme, the subject and others pretended to work for technology companies and contacted victims through computer pop-ups and telephone calls. Once contact was made, the subject and others induced victims to authorize payments under false pretenses and utilized remote desktop access applications to initiate unauthorized financial transactions from the victims' financial accounts. The IC3 provided ongoing assistance to the Philadelphia Field Office for this case.

RANSOMWARE

Ransomware is a form of malware targeting both human and technical weaknesses in an effort to make critical data and/or systems inaccessible. Ransomware is delivered through various vectors, including Remote Desktop Protocol, which allows computers to connect to each other across a network, and phishing.



In one scenario, spear phishing emails are sent to end users that result in the rapid encryption of sensitive files on a corporate network. When the victim organization determines it is no longer able to access its data, the cyber actor demands the payment of a ransom, typically in virtual currency. The actor will purportedly provide an avenue to the victim to regain access to its data once the ransom is paid.

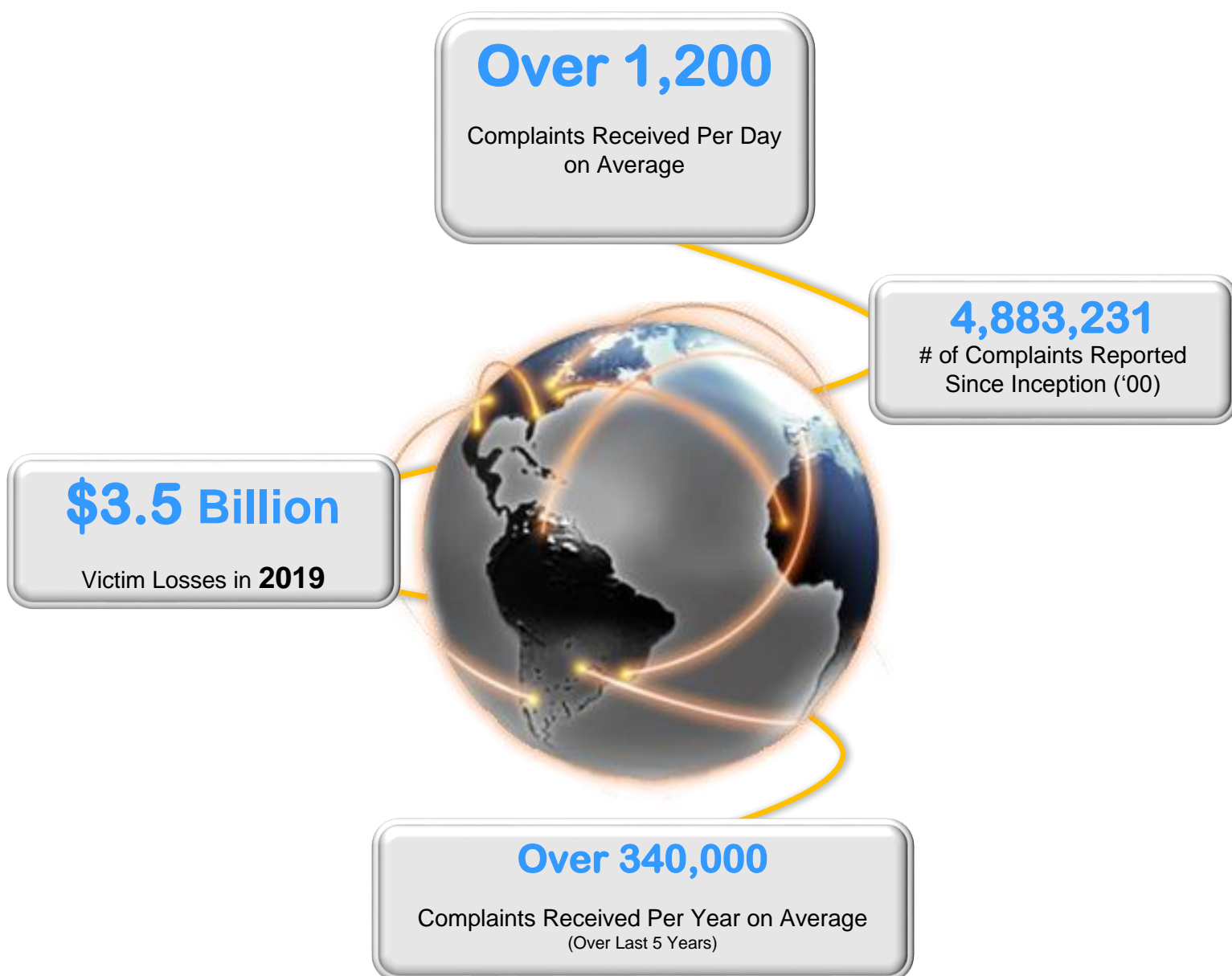
Recent iterations of this threat target specific organizations and their employees, making awareness and training a critical preventative measure.

The FBI advises not to pay the ransom to the adversary. Paying a ransom does not guarantee an organization will regain access to its data; in fact, some individuals or organizations were never provided with decryption keys after having paid a ransom. Paying a ransom emboldens the adversary to target other organizations for profit, and provides a lucrative environment for other criminals. While the FBI does not support paying a ransom, there is an understanding that when businesses are faced with an inability to function, executives will evaluate all options to protect their shareholders, employees, and customers.

The decision to pay the ransom should not dissuade someone from contacting the FBI. In all cases the FBI encourages organizations to contact a local FBI field office immediately to report a ransomware event and request assistance.

In 2019, the IC3 received 2,047 complaints identified as ransomware with adjusted losses of over \$8.9 million.

*IC3 by the Numbers*⁵



⁵ Accessibility description: Image depicts key statistics regarding complaints and victim loss. Total losses of \$3.5 billion were reported in 2019. The total number of complaints received since the year 2000 is 4,883,231. IC3 has received approximately 340,000 complaints per year on average over the last five years, or more than 1,200 complaints per day.

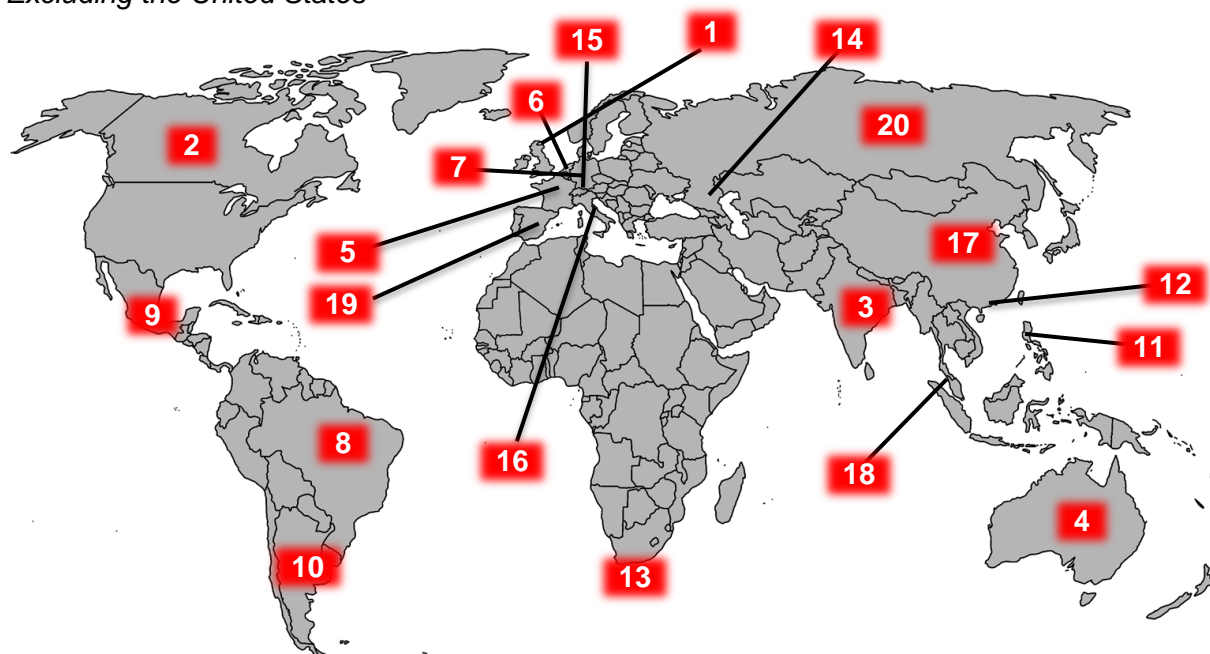
2019 VICTIMS BY AGE GROUP

Victims		
Age Range ⁶	Total Count	Total Loss
Under 20	10,724	\$421,169,232
20 - 29	44,496	\$174,673,470
30 - 39	52,820	\$332,208,189
40 - 49	51,864	\$529,231,267
50 - 59	50,608	\$589,624,844
Over 60	68,013	\$835,164,766

⁶ 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.

2019 - TOP 20 INTERNATIONAL VICTIM COUNTRIES

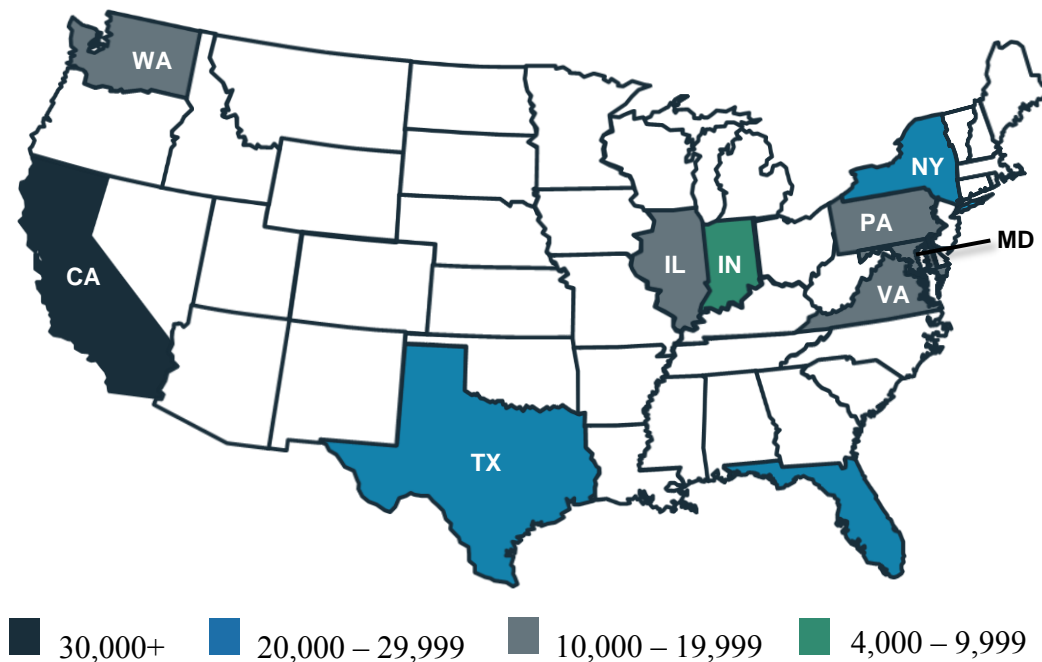
Excluding the United States⁷



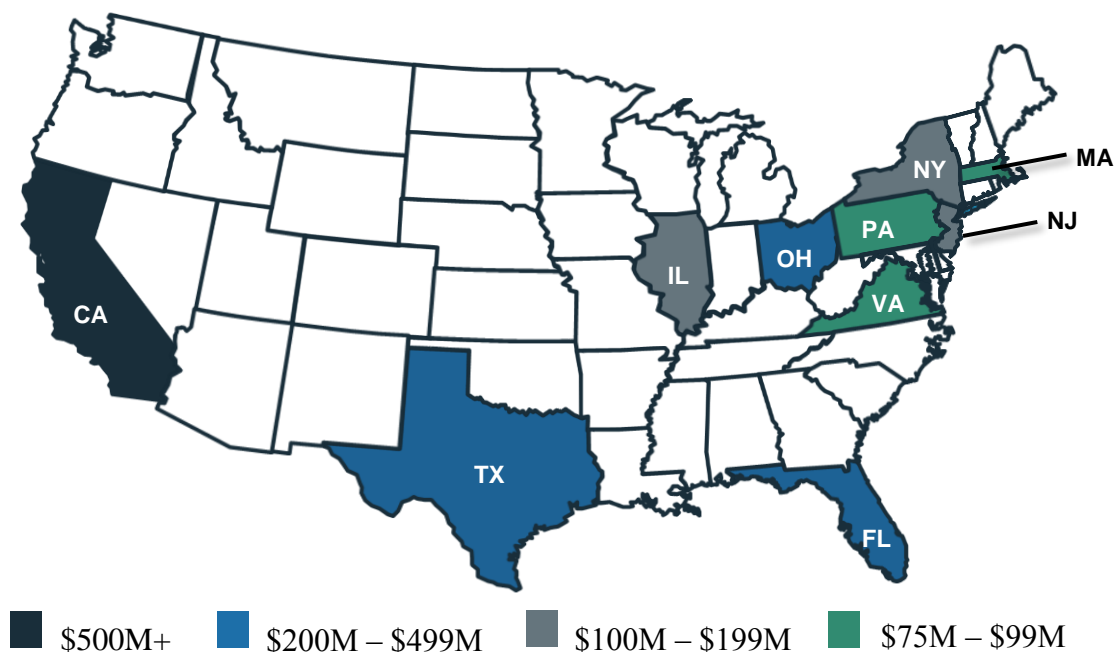
1. United Kingdom	93,796	6. Belgium	1,031	11. Philippines	561	16. Italy	428
2. Canada	3,721	7. Germany	850	12. Hong Kong	535	17. China	403
3. India	2,901	8. Brazil	628	13. South Africa	465	18. Malaysia	362
4. Australia	1,298	9. Mexico	605	14. Georgia	454	19. Spain	358
5. France	1,243	10. Argentina	578	15. Switzerland	438	20. Russian Federation	349

⁷ 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.

2019 - TOP 10 STATES BY NUMBER OF VICTIMS⁸



2019 - TOP 10 STATES BY VICTIM LOSS⁹



⁸ 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, Texas, Florida, New York, Washington, Pennsylvania, Virginia, Illinois, Maryland, and Indiana. Please see Appendix B for more information regarding IC3 data.

⁹ Accessibility description: Image depicts a map of the United States. The top 10 states based on reported victim loss are labeled. These include California, Texas, Florida, Ohio, New Jersey, Illinois, New York, Pennsylvania, Virginia, and Massachusetts. Please see Appendix B for more information regarding IC3 data.

2019 CRIME TYPES

By Victim Count			
Crime Type	Victims	Crime Type	Victims
Phishing/Vishing/Smishing/Pharming	114,702	Lottery/Sweepstakes/Inheritance	7,767
Non-Payment/Non-Delivery	61,832	Misrepresentation	5,975
Extortion	43,101	Investment	3,999
Personal Data Breach	38,218	IPR/Copyright and Counterfeit	3,892
Spoofing	25,789	Malware/Scareware/Virus	2,373
BEC/EAC	23,775	Ransomware	2,047
Confidence Fraud/Romance	19,473	Corporate Data Breach	1,795
Identity Theft	16,053	Denial of Service/TDoS	1,353
Harassment/Threats of Violence	15,502	Crimes Against Children	1,312
Overpayment	15,395	Re-shipping	929
Advanced Fee	14,607	Civil Matter	908
Employment	14,493	Health Care Related	657
Credit Card Fraud	14,378	Charity	407
Government Impersonation	13,873	Gambling	262
Tech Support	13,633	Terrorism	61
Real Estate/Rental	11,677	Hacktivist	39
Other	10,842		

Descriptors*		
Social Media	29,093	*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.
Virtual Currency	29,313	

2019 Crime Types *Continued*

By Victim Loss

Crime Type	Loss	Crime Type	Loss
BEC/EAC	\$1,776,549,688	Employment	\$42,618,705
Confidence Fraud/Romance	\$475,014,032	Civil Matter	\$20,242,867
Spoofing	\$300,478,433	Harassment/Threats of Violence	\$19,866,654
Investment	\$222,186,195	Misrepresentation	\$12,371,573
Real Estate/Rental	\$221,365,911	IPR/Copyright and Counterfeit	\$10,293,307
Non-Payment/Non-Delivery	\$196,563,497	Ransomware	**\$8,965,847
Identity Theft	\$160,305,789	Denial of Service/TDoS	\$7,598,198
Government Impersonation	\$124,292,606	Charity	\$2,214,383
Personal Data Breach	\$120,102,501	Malware/Scareware/Virus	\$2,009,119
Credit Card Fraud	\$111,491,163	Re-shipping	\$1,772,692
Extortion	\$107,498,956	Gambling	\$1,458,118
Advanced Fee	\$100,602,297	Health Care Related	\$1,128,838
Other	\$66,223,160	Crimes Against Children	\$975,311
Phishing/Vishing/Smishing/Pharming	\$57,836,379	Hacktivist	\$129,000
Overpayment	\$55,820,212	Terrorism	\$49,589
Tech Support	\$54,041,053		
Corporate Data Breach	\$53,398,278		
Lottery/Sweepstakes/Inheritance	\$48,642,332		

Descriptors*

Social Media	\$78,775,408	*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.
Virtual Currency	\$159,329,101	

**** 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.**

2019 OVERALL STATE STATISTICS

Count by Victim per State*

Rank	State	Victims	Rank	State	Victims
1	California	50,132	30	Utah	3,304
2	Florida	27,178	31	Kentucky	3,083
3	Texas	27,178	32	Oklahoma	2,887
4	New York	21,371	33	New Mexico	2,037
5	Washington	13,095	34	Arkansas	1,991
6	Maryland	11,709	35	Kansas	1,970
7	Virginia	11,674	36	Mississippi	1,654
8	Pennsylvania	10,914	37	Idaho	1,485
9	Illinois	10,337	38	Alaska	1,451
10	Indiana	9,746	39	District of Columbia	1,407
11	Colorado	9,689	40	Hawaii	1,396
12	Ohio	9,321	41	Nebraska	1,350
13	Georgia	9,074	42	West Virginia	1,227
14	New Jersey	9,067	43	New Hampshire	1,155
15	Michigan	8,249	44	Delaware	1,062
16	North Carolina	8,223	45	Rhode Island	1,011
17	Arizona	7,795	46	Montana	967
18	Massachusetts	6,492	47	Maine	880
19	Nevada	6,381	48	Puerto Rico	839
20	Wisconsin	6,378	49	Wyoming	550
21	Tennessee	5,586	50	Vermont	500
22	Iowa	5,094	51	North Dakota	489
23	Missouri	5,083	52	South Dakota	473
24	Oregon	4,813	53	U.S. Virgin Islands	75
25	South Carolina	4,541	54	Guam	71
26	Connecticut	4,412	55	U.S. Minor Outlying Islands	46
27	Minnesota	4,388	56	American Samoa	23
28	Alabama	4,108	57	Northern Marina Islands	11
29	Louisiana	3,804			

***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.

2019 Overall State Statistics *Continued*

Total Losses by Victim per State*					
Rank	State	Loss	Rank	State	Loss
1	California	\$573,624,151	30	Wisconsin	\$21,576,109
2	Florida	\$293,445,963	31	Alabama	\$20,586,392
3	Ohio	\$264,663,456	32	South Carolina	\$20,186,041
4	Texas	\$221,535,479	33	New Mexico	\$17,983,833
5	New York	\$198,765,769	34	Kentucky	\$17,014,895
6	Illinois	\$107,152,415	35	Kansas	\$16,107,619
7	New Jersey	\$106,474,464	36	Nebraska	\$14,596,769
8	Pennsylvania	\$94,281,611	37	Idaho	\$12,627,102
9	Virginia	\$92,467,791	38	District of Columbia	\$12,175,460
10	Massachusetts	\$84,173,754	39	Rhode Island	\$10,182,363
11	Georgia	\$79,732,460	40	Mississippi	\$10,129,650
12	Washington	\$71,286,037	41	Hawaii	\$10,005,566
13	Colorado	\$65,118,524	42	Alaska	\$9,654,238
14	Maryland	\$52,830,779	43	Montana	\$8,295,010
15	North Carolina	\$48,425,764	44	Wyoming	\$8,138,463
16	Michigan	\$47,122,182	45	Puerto Rico	\$7,668,517
17	Arizona	\$47,058,842	46	New Hampshire	\$7,284,552
18	Utah	\$46,458,273	47	Delaware	\$6,105,401
19	Minnesota	\$39,421,520	48	West Virginia	\$5,442,899
20	Oregon	\$37,088,022	49	North Dakota	\$4,527,733
21	Nevada	\$35,720,611	50	Maine	\$3,267,370
22	Connecticut	\$33,789,138	51	South Dakota	\$3,086,846
23	Tennessee	\$33,052,233	52	Vermont	\$2,329,973
24	Oklahoma	\$28,556,326	53	U.S. Virgin Islands	\$2,113,723
25	Iowa	\$27,919,567	54	Guam	\$898,265
26	Missouri	\$27,290,803	55	U.S. Minor Outlying Islands	\$143,012
27	Louisiana	\$24,214,439	56	American Samoa	\$16,359
28	Indiana	\$24,030,998	57	Northern Mariana Islands	\$2,300
29	Arkansas	\$22,681,002			

***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.

2019 Overall State Statistics *Continued*

Count by Subject per State*					
Rank	State	Subjects	Rank	State	Subjects
1	California	17,517	30	New Mexico	943
2	Florida	11,047	31	Oklahoma	940
3	Texas	10,093	32	Utah	934
4	New York	8,345	33	Wisconsin	933
5	Maryland	7,228	34	Connecticut	846
6	Virginia	4,829	35	Montana	832
7	Illinois	3,465	36	Kentucky	789
8	Georgia	3,325	37	District of Columbia	779
9	Washington	3,317	38	Mississippi	748
10	New Jersey	3,312	39	Iowa	612
11	Pennsylvania	2,793	40	Hawaii	547
12	Ohio	2,506	41	Arkansas	532
13	Nevada	2,481	42	Puerto Rico	476
14	North Carolina	2,259	43	Idaho	432
15	Tennessee	2,186	44	North Dakota	377
16	Arizona	2,119	45	Maine	312
17	Michigan	2,029	46	New Hampshire	264
18	Indiana	1,933	47	West Virginia	262
19	Colorado	1,848	48	Rhode Island	241
20	Massachusetts	1,480	49	Alaska	222
21	Missouri	1,376	50	Wyoming	175
22	Minnesota	1,276	51	South Dakota	133
23	Oregon	1,240	52	Vermont	131
24	Nebraska	1,201	53	U.S. Minor Outlying Islands	19
25	South Carolina	1,137	54	U.S. Virgin Islands	12
26	Louisiana	1,103	55	Guam	11
27	Alabama	1,049	56	American Samoa	7
28	Kansas	976	57	Northern Mariana Islands	1
29	Delaware	948			

***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.

2019 Overall State Statistics *Continued***Subject Earnings per Destination State***

Rank	State	Loss	Rank	State	Loss
1	Indiana	\$231,002,496	30	Utah	\$7,912,016
2	California	\$183,168,069	31	Missouri	\$6,432,347
3	Texas	\$126,282,907	32	Idaho	\$5,892,792
4	New York	\$95,996,214	33	Iowa	\$5,763,972
5	Florida	\$95,910,080	34	Louisiana	\$4,958,777
6	Georgia	\$55,338,192	35	Hawaii	\$4,761,209
7	Illinois	\$48,100,395	36	Kentucky	\$4,704,251
8	New Jersey	\$32,048,215	37	New Hampshire	\$3,520,598
9	Washington	\$31,928,985	38	Montana	\$3,235,197
10	Pennsylvania	\$29,787,276	39	Arkansas	\$3,206,417
11	Arizona	\$25,960,706	40	West Virginia	\$2,754,324
12	Virginia	\$24,879,452	41	Nebraska	\$2,614,627
13	Maryland	\$23,977,444	42	Delaware	\$2,548,620
14	Massachusetts	\$20,192,012	43	Mississippi	\$2,518,412
15	Connecticut	\$17,845,526	44	Rhode Island	\$2,105,153
16	Colorado	\$16,678,494	45	New Mexico	\$1,889,690
17	Tennessee	\$15,532,247	46	Maine	\$1,656,784
18	Ohio	\$14,569,674	47	Wyoming	\$1,547,198
19	North Carolina	\$13,983,462	48	North Dakota	\$1,452,038
20	Nevada	\$13,497,823	49	Alaska	\$1,431,485
21	Michigan	\$13,466,196	50	South Dakota	\$975,629
22	Oklahoma	\$12,082,341	51	Puerto Rico	\$852,121
23	Minnesota	\$11,518,980	52	Vermont	\$686,424
24	Wisconsin	\$10,722,858	53	U.S. Minor Outlying Islands	\$77,491
25	Oregon	\$9,325,763	54	U.S. Virgin Islands	\$27,748
26	Kansas	\$8,954,238	55	Guam	\$15,014
27	South Carolina	\$8,454,695	56	American Samoa	\$12,100
28	District of Columbia	\$8,280,731	57	Northern Mariana Islands	\$0.00
29	Alabama	\$7,988,933			

***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: CRIME TYPE 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: In advanced fee schemes, the perpetrator informs a victim that the victim has qualified for a large financial loan or has won a large financial award, but must first pay the perpetrator taxes or fees in order to access the loan or award. The victim pays the advance fee, but never receives the promised money.

Business Email Compromise/Email Account Compromise: BEC is a scam targeting businesses working with foreign suppliers and/or businesses regularly performing wire transfer payments. EAC is a similar scam that 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 lawsuits are any disputes formally submitted to a court that is not criminal.

Confidence/Romance Fraud: A perpetrator deceives a victim into believing the perpetrator and the victim have a trust relationship, whether family, friendly or romantic. As a result of that belief, the victim is persuaded to send money, personal and financial information, or items of value to the perpetrator or to launder money on behalf of the perpetrator. Some variations of this scheme are romance/dating scams or the grandparent scam.

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 fraud committed using a credit card or any similar payment mechanism 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 service with multiple requests, slowing down or interrupting service.

Employment: Individuals believe they are legitimately employed, and lose 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, usually involving health care providers, companies, or individuals. Schemes may include offers for fake insurance cards, health insurance marketplace assistance, or stolen health information, or may involve medications, supplements, weight loss products, or diversion/pill mill practices. These scams are often initiated through spam email, Internet advertisements, links in forums or social media, and fraudulent websites.

IPR/Copyright and Counterfeit: The theft and illegal use of others' ideas, inventions, and creative expressions, to include everything from trade secrets and proprietary products to parts, movies, music, and software.

Identity Theft/Account Takeover: Identify theft involves a perpetrator stealing another person's personal identifying information, such as name or Social Security number, without permission to commit fraud. Account Takeover is when a perpetrator obtains account information to perpetrate fraud on existing accounts.

Investment: A 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. Variations of this scam include retirement schemes, Ponzi schemes and pyramid schemes.

Lottery/Sweepstakes/Inheritance: Individuals are contacted about winning a lottery or sweepstakes they never entered, or to collect on an inheritance from an unknown relative and are asked to pay a tax or fee in order to receive their award.

Malware/Scareware/Virus: Software or code intended to damage or disable computers and computer systems. Sometimes scare tactics are used by the perpetrators to solicit funds.

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 or spill of personal data that is released from a secure location to an untrusted environment. It may also refer to 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: 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 purchased through fraudulent means and subsequently repackage the merchandise for shipment, usually abroad.

Real Estate/Rental: Fraud involving real estate, 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 robo-calls; spoofed emails sending mass spam; forged websites used to mislead and gather personal information. Spoofing is 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: Attempts to gain access to a victim's electronic device by falsely claiming to offer tech support, usually for a well-known company. Scammer asks for remote access to the victim's device to cleanup viruses or malware or to facilitate a refund for prior support services.

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.



INTERNET CRIME REPORT 2020

2020 Internet Crime Report

TABLE OF CONTENTS

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

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 into 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



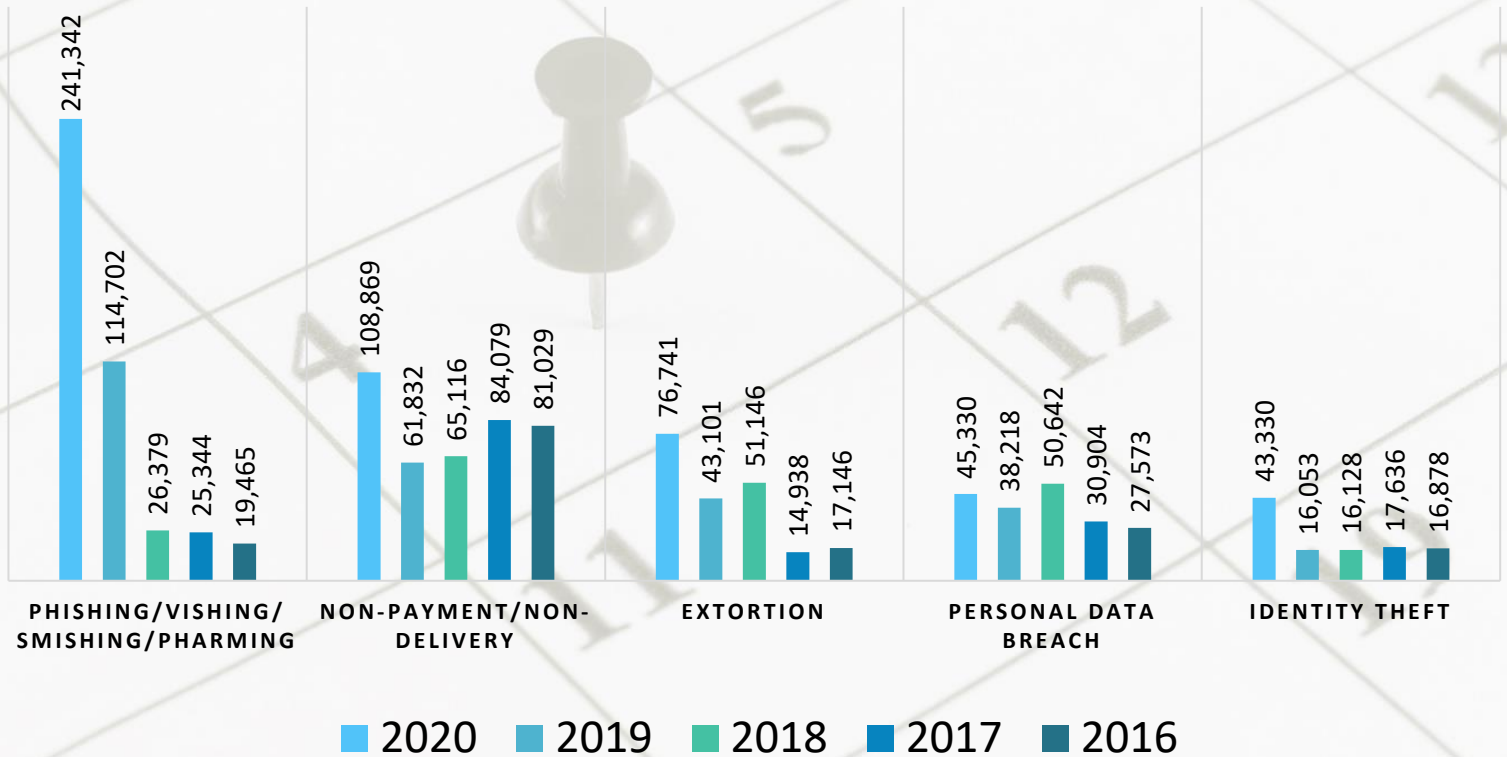
\$13.3 Billion TOTAL LOSSES*

(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 Statistics²

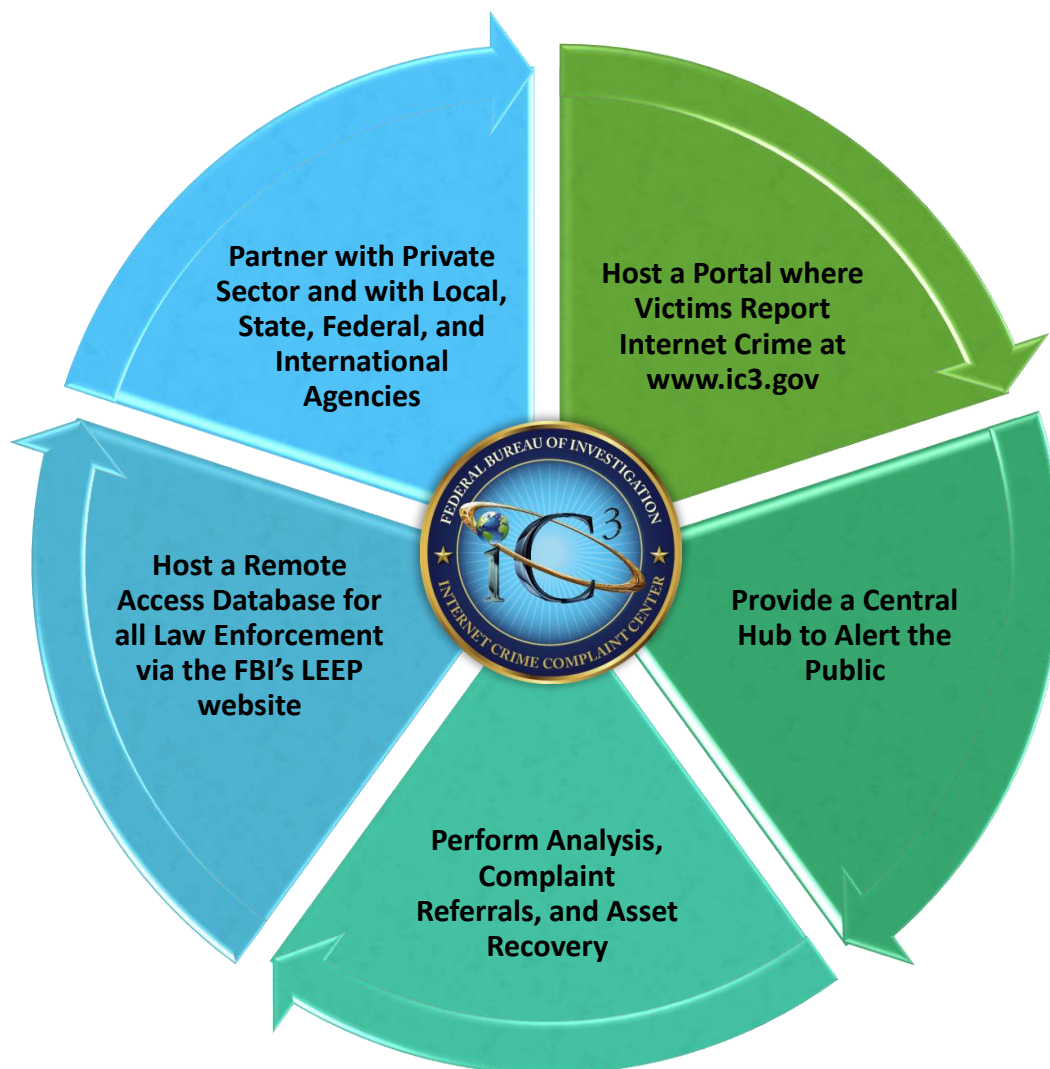
2020 - Top 5 Crime Type Comparison *Last Five Years*



² 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 Crime³

WHAT WE DO



³ 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.

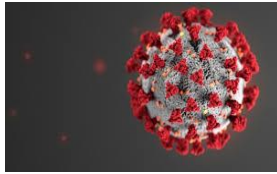
IC3 Core Functions

 <p>IC3 Core Functions⁴</p>			
COLLECTION ANALYSIS PUBLIC AWARENESS REFERRALS			
<p>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 www.ic3.gov. 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.</p>	<p>The IC3 reviews and analyzes data submitted through its website to identify emerging threats and new trends.</p>	<p>Public service announcements, industry alerts, and other publications outlining specific scams are posted to the www.ic3.gov 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.</p>	<p>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.</p>

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.

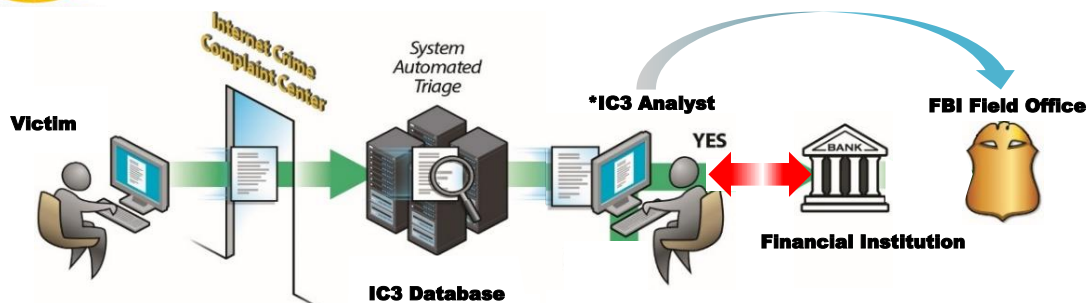
As the fraudsters have become more sophisticated, the BEC/EAC scheme has evolved in kind. In 2013, BEC/EAC scams routinely began with the hacking or spoofing of the email accounts of chief executive officers or chief financial officers, and fraudulent emails were sent requesting wire payments be sent 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*⁵

*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.

⁵ 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 sent 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



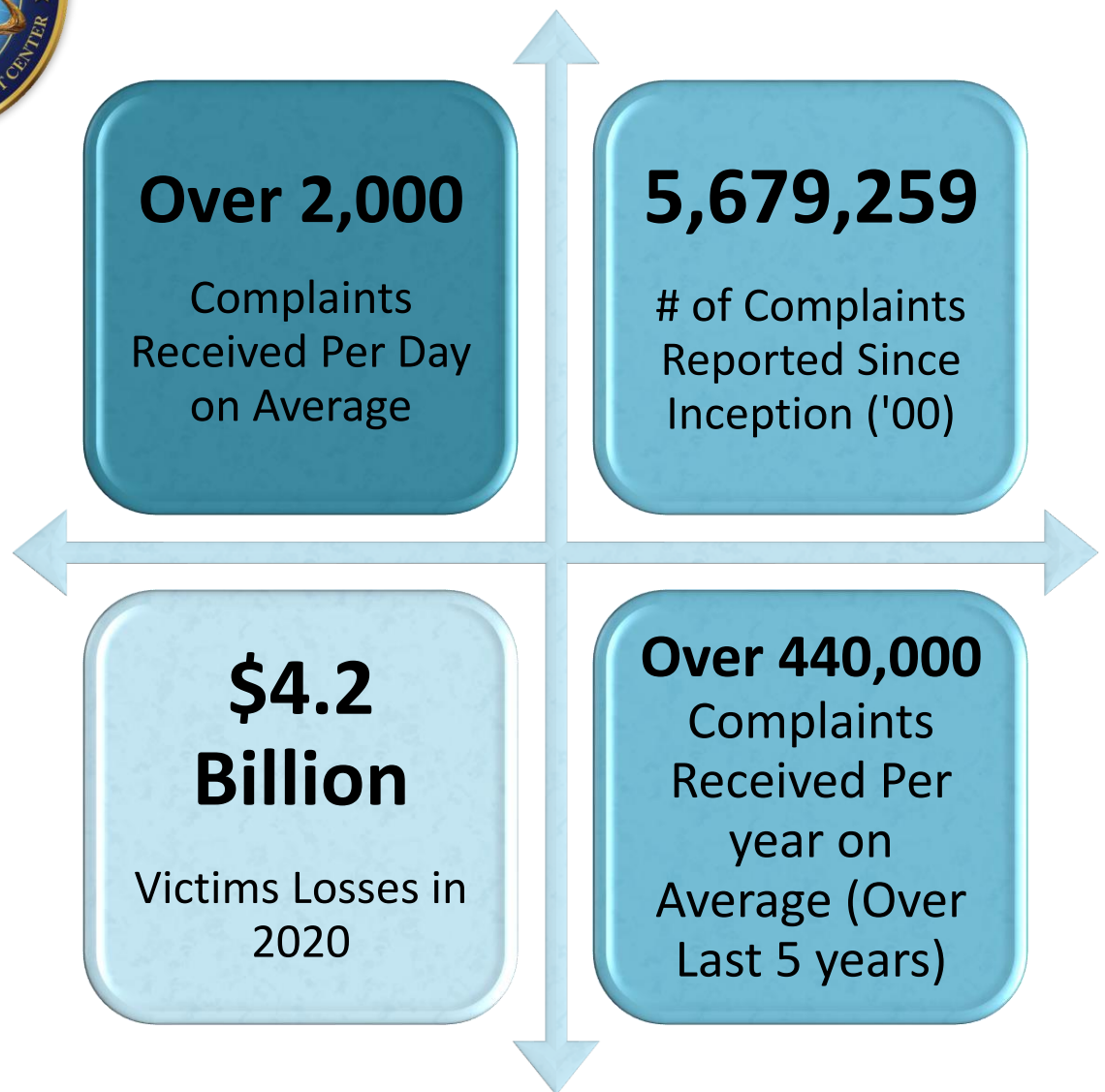
In 2020, the IC3 received 2,474 complaints identified as ransomware with adjusted losses of over \$29.1 million. Ransomware is a type of malicious software, or malware, that encrypts data on a computer making it unusable. A malicious cyber criminal holds the data hostage until the ransom is paid. If 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.

IC3 by the Numbers⁶



⁶ 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.

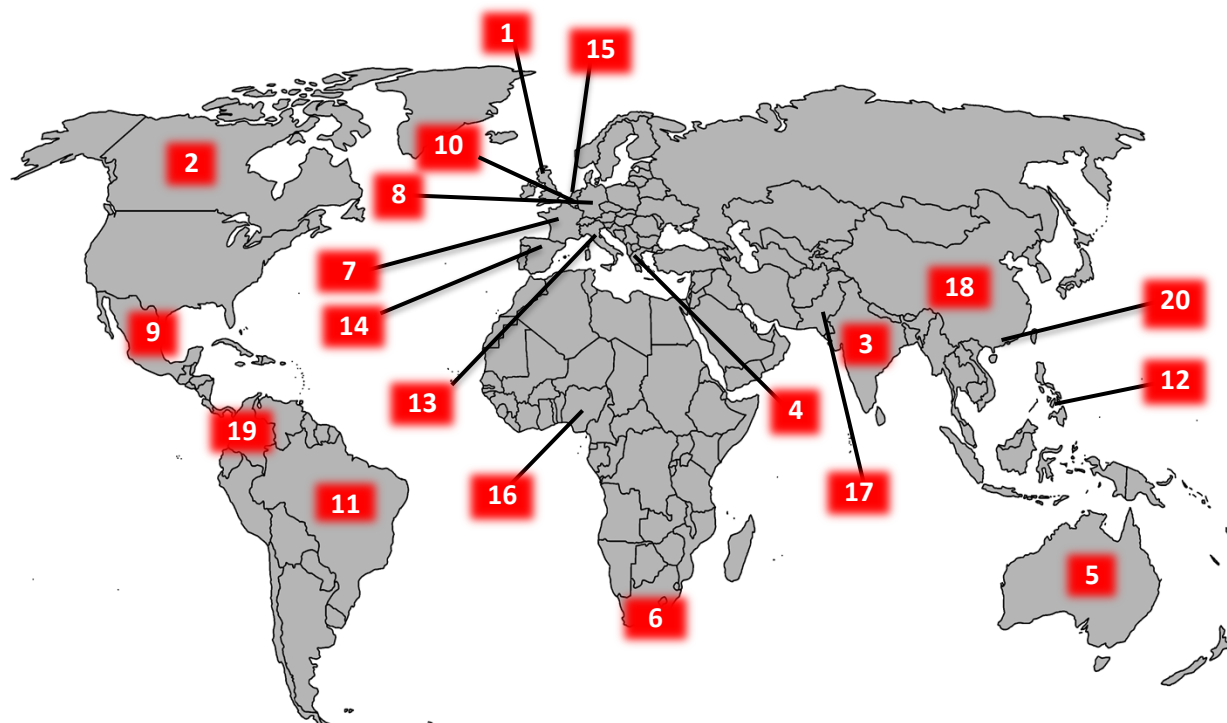
2020 VICTIMS BY AGE GROUP

Victims		
Age Range ⁷	Total Count	Total Loss
Under 20	23,186	\$70,980,763
20 - 29	70,791	\$197,402,240
30 - 39	88,364	\$492,176,845
40 - 49	91,568	\$717,161,726
50 - 59	85,967	\$847,948,101
Over 60	105,301	\$966,062,236

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

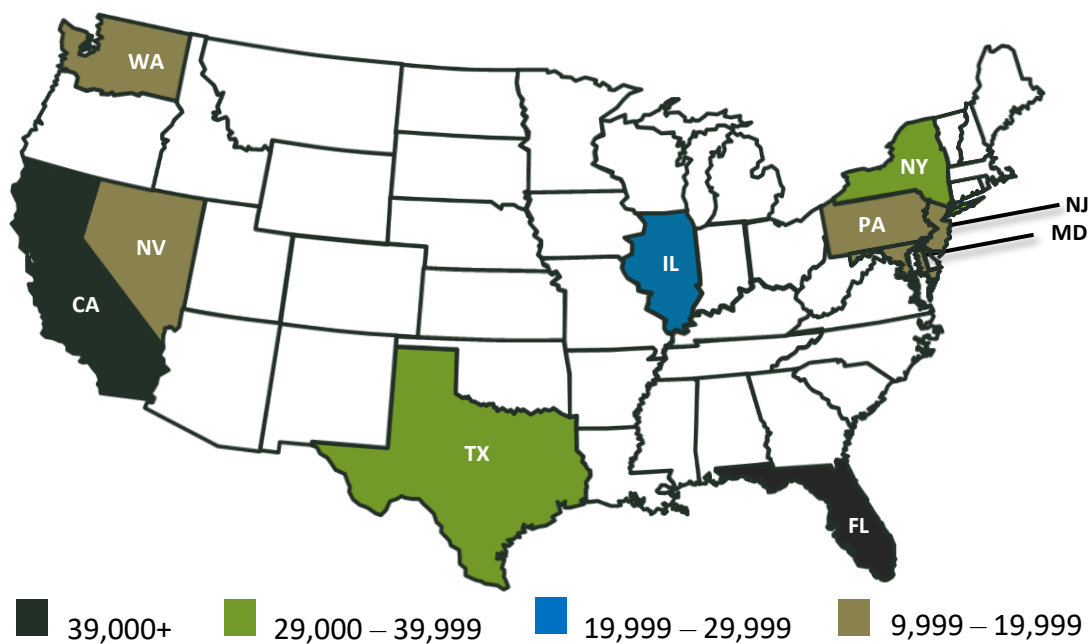
Excluding the United States⁸



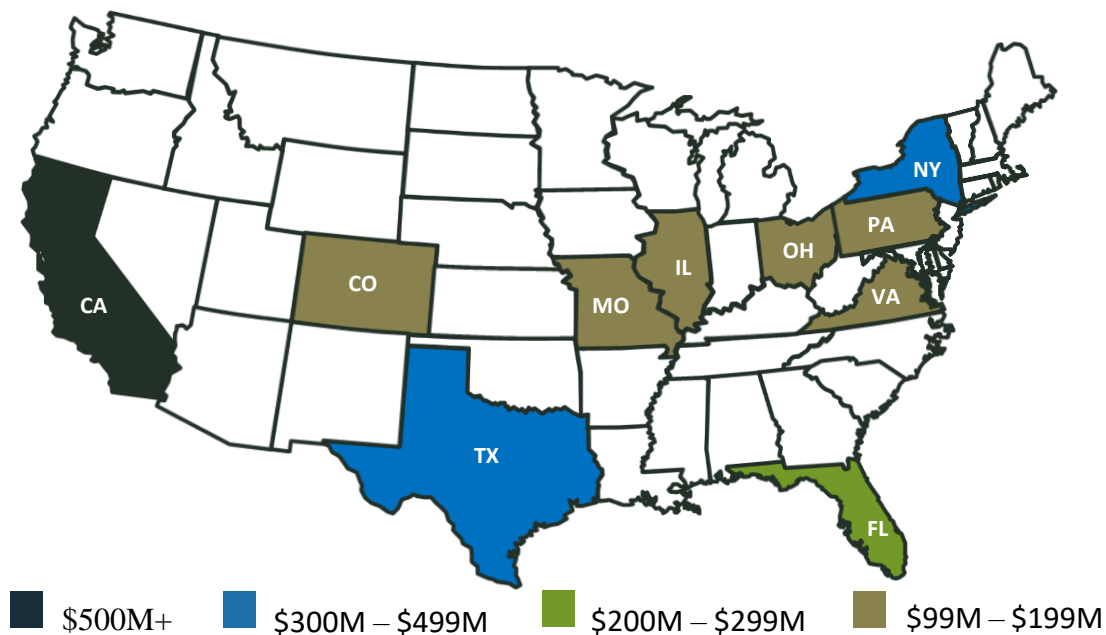
1. United Kingdom	216,633	6. South Africa	1,754	11. Brazil	951	16. Nigeria	443
2. Canada	5,399	7. France	1,640	12. Philippines	898	17. Pakistan	443
3. India	2,930	8. Germany	1,578	13. Italy	728	18. China	442
4. Greece	2,314	9. Mexico	1,164	14. Spain	618	19. Colombia	418
5. Australia	1,807	10. Belgium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

⁸ 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 VICTIMS⁹



2020 - TOP 10 STATES BY VICTIM LOSS¹⁰



⁹ 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.

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

Descriptors*		
Social Media	35,439	*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.
Virtual Currency	35,229	

2020 Crime Types *Continued*

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

Descriptors*		
Social Media	\$155,323,073	*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.
Virtual Currency	\$246,212,432	

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

Last 3 Year Complaint Loss Comparison *Continued*

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

2020 Overall State Statistics

Victim per State*

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

***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*					
Rank	State	Loss	Rank	State	Loss
1	California	\$621,452,320	30	South Carolina	\$25,244,978
2	New York	\$415,812,917	31	New Mexico	\$23,903,594
3	Texas	\$313,565,225	32	Iowa	\$21,396,701
4	Florida	\$295,032,829	33	Oklahoma	\$20,748,692
5	Ohio	\$170,171,951	34	Kansas	\$19,157,289
6	Illinois	\$150,496,678	35	District of Columbia	\$18,942,722
7	Missouri	\$115,913,584	36	Mississippi	\$18,111,738
8	Pennsylvania	\$108,506,204	37	Arkansas	\$17,371,515
9	Virginia	\$101,661,604	38	Hawaii	\$13,671,531
10	Colorado	\$100,663,897	39	Puerto Rico	\$13,275,104
11	Georgia	\$98,762,523	40	Kentucky	\$12,590,784
12	New Jersey	\$98,727,053	41	Nebraska	\$11,799,640
13	Massachusetts	\$97,583,753	42	Idaho	\$11,670,650
14	Washington	\$88,020,254	43	American Samoa	\$7,806,373
15	Michigan	\$83,999,442	44	Rhode Island	\$7,669,670
16	Arizona	\$72,128,637	45	Alaska	\$7,342,743
17	North Carolina	\$69,409,152	46	Maine	\$7,073,260
18	Maryland	\$62,473,193	47	Delaware	\$6,486,617
19	Minnesota	\$58,341,798	48	Montana	\$5,669,293
20	Utah	\$47,113,946	49	Wyoming	\$5,096,704
21	Nevada	\$44,383,452	50	New Hampshire	\$4,949,296
22	Connecticut	\$41,311,798	51	West Virginia	\$4,823,786
23	Tennessee	\$40,191,616	52	Vermont	\$4,175,799
24	Oregon	\$38,389,702	53	South Dakota	\$3,208,241
25	Wisconsin	\$36,081,681	54	Virgin Islands, U.S.	\$620,962
26	Indiana	\$35,180,105	55	Guam	\$259,338
27	Alabama	\$27,549,157	56	U.S. Minor Outlying Islands	\$201,022
28	Louisiana	\$26,717,928	57	Northern Mariana Islands	\$67,403
29	North Dakota	\$25,804,940			

***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*

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

***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*

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

***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 robo-calls; 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.

Executive Order 13694 of April 1, 2015

Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities

By the authority vested in me as President by the Constitution and the laws of the United States of America, including the International Emergency Economic Powers Act (50 U.S.C. 1701 *et seq.*) (IEEPA), the National Emergencies Act (50 U.S.C. 1601 *et seq.*) (NEA), section 212(f) of the Immigration and Nationality Act of 1952 (8 U.S.C. 1182(f)), and section 301 of title 3, United States Code,

I, BARACK OBAMA, President of the United States of America, find that the increasing prevalence and severity of malicious cyber-enabled activities originating from, or directed by persons located, in whole or in substantial part, outside the United States constitute an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States. I hereby declare a national emergency to deal with this threat.

Accordingly, I hereby order:

Section 1. (a) All property and interests in property that are in the United States, that hereafter come within the United States, or that are or hereafter come within the possession or control of any United States person of the following persons are blocked and may not be transferred, paid, exported, withdrawn, or otherwise dealt in:

(i) any person determined by the Secretary of the Treasury, in consultation with the Attorney General and the Secretary of State, to be responsible for or complicit in, or to have engaged in, directly or indirectly, cyber-enabled activities originating from, or directed by persons located, in whole or in substantial part, outside the United States that are reasonably likely to result in, or have materially contributed to, a significant threat to the national security, foreign policy, or economic health or financial stability of the United States and that have the purpose or effect of:

(A) harming, or otherwise significantly compromising the provision of services by, a computer or network of computers that support one or more entities in a critical infrastructure sector;

(B) significantly compromising the provision of services by one or more entities in a critical infrastructure sector;

(C) causing a significant disruption to the availability of a computer or network of computers; or

(D) causing a significant misappropriation of funds or economic resources, trade secrets, personal identifiers, or financial information for commercial or competitive advantage or private financial gain; or

(ii) any person determined by the Secretary of the Treasury, in consultation with the Attorney General and the Secretary of State:

(A) to be responsible for or complicit in, or to have engaged in, the receipt or use for commercial or competitive advantage or private financial gain, or by a commercial entity, outside the United States of trade secrets misappropriated through cyber-enabled means, knowing they

have been misappropriated, where the misappropriation of such trade secrets is reasonably likely to result in, or has materially contributed to, a significant threat to the national security, foreign policy, or economic health or financial stability of the United States;

(B) to have materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services in support of, any activity described in subsections (a)(i) or (a)(ii)(A) of this section or any person whose property and interests in property are blocked pursuant to this order;

(C) to be owned or controlled by, or to have acted or purported to act for or on behalf of, directly or indirectly, any person whose property and interests in property are blocked pursuant to this order; or

(D) to have attempted to engage in any of the activities described in subsections (a)(i) and (a)(ii)(A)–(C) of this section.

(b) The prohibitions in subsection (a) of this section apply except to the extent provided by statutes, or in regulations, orders, directives, or licenses that may be issued pursuant to this order, and notwithstanding any contract entered into or any license or permit granted prior to the effective date of this order.

Sec. 2. I hereby determine that the making of donations of the type of articles specified in section 203(b)(2) of IEEPA (50 U.S.C. 1702(b)(2)) by, to, or for the benefit of any person whose property and interests in property are blocked pursuant to section 1 of this order would seriously impair my ability to deal with the national emergency declared in this order, and I hereby prohibit such donations as provided by section 1 of this order.

Sec. 3. The prohibitions in section 1 of this order include but are not limited to:

(a) the making of any contribution or provision of funds, goods, or services by, to, or for the benefit of any person whose property and interests in property are blocked pursuant to this order; and

(b) the receipt of any contribution or provision of funds, goods, or services from any such person.

Sec. 4. I hereby find that the unrestricted immigrant and nonimmigrant entry into the United States of aliens determined to meet one or more of the criteria in section 1(a) of this order would be detrimental to the interests of the United States, and I hereby suspend entry into the United States, as immigrants or nonimmigrants, of such persons. Such persons shall be treated as persons covered by section 1 of Proclamation 8693 of July 24, 2011 (Suspension of Entry of Aliens Subject to United Nations Security Council Travel Bans and International Emergency Economic Powers Act Sanctions).

Sec. 5. (a) Any transaction that evades or avoids, has the purpose of evading or avoiding, causes a violation of, or attempts to violate any of the prohibitions set forth in this order is prohibited.

(b) Any conspiracy formed to violate any of the prohibitions set forth in this order is prohibited.

Sec. 6. For the purposes of this order:

(a) the term “person” means an individual or entity;

(b) the term “entity” means a partnership, association, trust, joint venture, corporation, group, subgroup, or other organization;

(c) the term “United States person” means any United States citizen, permanent resident alien, entity organized under the laws of the United States or any jurisdiction within the United States (including foreign branches), or any person in the United States;

(d) the term “critical infrastructure sector” means any of the designated critical infrastructure sectors identified in Presidential Policy Directive 21; and

(e) the term “misappropriation” includes any taking or obtaining by improper means, without permission or consent, or under false pretenses.

Sec. 7. For those persons whose property and interests in property are blocked pursuant to this order who might have a constitutional presence in the United States, I find that because of the ability to transfer funds or other assets instantaneously, prior notice to such persons of measures to be taken pursuant to this order would render those measures ineffectual. I therefore determine that for these measures to be effective in addressing the national emergency declared in this order, there need be no prior notice of a listing or determination made pursuant to section 1 of this order.

Sec. 8. The Secretary of the Treasury, in consultation with the Attorney General and the Secretary of State, is hereby authorized to take such actions, including the promulgation of rules and regulations, and to employ all powers granted to the President by IEEPA as may be necessary to carry out the purposes of this order. The Secretary of the Treasury may redelegate any of these functions to other officers and agencies of the United States Government consistent with applicable law. All agencies of the United States Government are hereby directed to take all appropriate measures within their authority to carry out the provisions of this order.

Sec. 9. The Secretary of the Treasury, in consultation with the Attorney General and the Secretary of State, is hereby authorized to submit the recurring and final reports to the Congress on the national emergency declared in this order, consistent with section 401(c) of the NEA (50 U.S.C. 1641(c)) and section 204(c) of IEEPA (50 U.S.C. 1703(c)).

Sec. 10. 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.

BARACK OBAMA

The White House,
April 1, 2015.

Presidential Documents

Title 3—

Executive Order 13757 of December 28, 2016

The President

Taking Additional Steps to Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities

By the authority vested in me as President by the Constitution and the laws of the United States of America, including the International Emergency Economic Powers Act (50 U.S.C. 1701 *et seq.*) (IEEPA), the National Emergencies Act (50 U.S.C. 1601 *et seq.*) (NEA), and section 301 of title 3, United States Code,

I, BARACK OBAMA, President of the United States of America, in order to take additional steps to deal with the national emergency with respect to significant malicious cyber-enabled activities declared in Executive Order 13694 of April 1, 2015, and in view of the increasing use of such activities to undermine democratic processes or institutions, hereby order:

Section 1. Section 1(a) of Executive Order 13694 is hereby amended to read as follows:

“Section 1. (a) All property and interests in property that are in the United States, that hereafter come within the United States, or that are or hereafter come within the possession or control of any United States person of the following persons are blocked and may not be transferred, paid, exported, withdrawn, or otherwise dealt in:

(i) the persons listed in the Annex to this order;

(ii) any person determined by the Secretary of the Treasury, in consultation with the Attorney General and the Secretary of State, to be responsible for or complicit in, or to have engaged in, directly or indirectly, cyber-enabled activities originating from, or directed by persons located, in whole or in substantial part, outside the United States that are reasonably likely to result in, or have materially contributed to, a significant threat to the national security, foreign policy, or economic health or financial stability of the United States and that have the purpose or effect of:

(A) harming, or otherwise significantly compromising the provision of services by, a computer or network of computers that support one or more entities in a critical infrastructure sector;

(B) significantly compromising the provision of services by one or more entities in a critical infrastructure sector;

(C) causing a significant disruption to the availability of a computer or network of computers;

(D) causing a significant misappropriation of funds or economic resources, trade secrets, personal identifiers, or financial information for commercial or competitive advantage or private financial gain; or

(E) tampering with, altering, or causing a misappropriation of information with the purpose or effect of interfering with or undermining election processes or institutions; and

(iii) any person determined by the Secretary of the Treasury, in consultation with the Attorney General and the Secretary of State:

(A) to be responsible for or complicit in, or to have engaged in, the receipt or use for commercial or competitive advantage or private financial gain, or by a commercial entity, outside the United States of trade secrets

misappropriated through cyber-enabled means, knowing they have been misappropriated, where the misappropriation of such trade secrets is reasonably likely to result in, or has materially contributed to, a significant threat to the national security, foreign policy, or economy of the United States;

(B) to have materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services to or in support of, any activity described in subsections (a)(ii) or (a)(iii)(A) of this section or any person whose property and interests in property are blocked pursuant to this order;

(C) to be owned or controlled by, or to have acted or purported to act for or on behalf of, directly or indirectly, any person whose property and interests in property are blocked pursuant to this order; or

(D) to have attempted to engage in any of the activities described in subsections (a)(ii) and (a)(iii)(A)–(C) of this section.”

Sec. 2. Executive Order 13694 is further amended by adding as an Annex to Executive Order 13694 the Annex to this order.

Sec. 3. Executive Order 13694 is further amended by redesignating section 10 as section 11 and adding a new section 10 to read as follows:

“Sec. 10. The Secretary of the Treasury, in consultation with the Attorney General and the Secretary of State, is hereby authorized to determine that circumstances no longer warrant the blocking of the property and interests in property of a person listed in the Annex to this order, and to take necessary action to give effect to that determination.”

Sec. 4. 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.

Sec. 5. This order is effective at 12:01 a.m. eastern standard time on December 29, 2016.

A handwritten signature in black ink, appearing to be "Donald Trump", with a large circular flourish at the end.

THE WHITE HOUSE,
December 28, 2016.

Annex**Entities**

1. Main Intelligence Directorate (a.k.a. Glavnoe Razvedyvatel'noe Upravlenie) (a.k.a. GRU); Moscow, Russia
2. Federal Security Service (a.k.a. Federalnaya Sluzhba Bezopasnosti) (a.k.a FSB); Moscow, Russia
3. Special Technology Center (a.k.a. STLC, Ltd. Special Technology Center St. Petersburg); St. Petersburg, Russia
4. Zorsecurity (a.k.a. Esage Lab); Moscow, Russia
5. Autonomous Noncommercial Organization “Professional Association of Designers of Data Processing Systems” (a.k.a. ANO PO KSI); Moscow, Russia

Individuals

1. Igor Valentinovich Korobov; DOB Aug 3, 1956; nationality, Russian
2. Sergey Aleksandrovich Gizunov; DOB Oct 18, 1956; nationality, Russian
3. Igor Olegovich Kostyukov; DOB Feb 21, 1961; nationality, Russian
4. Vladimir Stepanovich Alexseyev; DOB Apr 24, 1961; nationality, Russian

OFAC

Office of Foreign Assets Control

CYBER-RELATED SANCTIONS PROGRAM

This document is explanatory only and does not have the force of law. This document does not supplement or modify applicable Executive orders, laws, or regulations.



Updated July 3, 2017

Contents

I. INTRODUCTION..... 3

II. OVERVIEW OF AUTHORITIES 3

III. PROHIBITED TRANSACTIONS 4

IV. AUTHORIZED TRANSACTIONS..... 4

V. ENFORCEMENT & PENALTIES 5

SANCTIONS AGAINST CERTAIN PERSONS ENGAGING IN SIGNIFICANT MALICIOUS CYBER-ENABLED ACTIVITIES

I. INTRODUCTION

The cyber-related sanctions program implemented by the Office of Foreign Assets Control (OFAC) began on April 1, 2015, when the President issued Executive Order (E.O.) 13694 and declared a national emergency to deal with the unusual and extraordinary threat to the national security, foreign policy, and economy of the United States constituted by the increasing prevalence and severity of malicious cyber-enabled activities originating from, or directed by persons located, in whole or in substantial part, outside the United States. This order authorizes, among other things, the imposition of sanctions against persons responsible for or complicit in, or to have engaged in, certain malicious cyber-enabled activities. On December 28, 2016, the President issued E.O. 13757, which amended E.O. 13694 by adding an Annex and authorizing sanctions related to interfering with or undermining election processes or institutions.

II. OVERVIEW OF AUTHORITIES

On April 1, 2015, the President issued [E.O. 13694](#) pursuant to, inter alia, the [International Emergency Economic Powers Act](#) (50 U.S.C. §§ 1701 et seq.) (IEEPA) and the [National Emergencies Act](#) (50 U.S.C. §§ 1601 et seq.). On December 28, 2016, the President issued [E.O. 13757](#), which amended E.O. 13694 to include an Annex of sanctioned persons and to expand the scope of cyber-enabled activities subject to sanctions.

The cyber-related sanctions pursuant to E.O. 13694, as amended, block the property and interests in property of persons that are determined by the Secretary of the Treasury, in consultation with the Attorney General and the Secretary of State:

- To be responsible for or complicit in, or to have engaged in, directly or indirectly, cyber-enabled activities originating from, or directed by persons located, in whole or in substantial part, outside the United States that are reasonably likely to result in, or have materially contributed to, a significant threat to the national security, foreign policy, or economic health or financial stability of the United States and that have the purpose or effect of:
 - 1) harming, or otherwise significantly compromising the provision of services by, a computer or network of computers that support one or more entities in a critical infrastructure sector;
 - 2) significantly compromising the provision of services by one or more entities in a critical infrastructure sector;
 - 3) causing a significant disruption to the availability of a computer or network of computers;
 - 4) causing a significant misappropriation of funds or economic resources, trade secrets, personal identifiers, or financial information for commercial or competitive advantage or private financial gain; or
 - 5) tampering with, altering, or causing a misappropriation of information with the purpose or effect of interfering with or undermining election processes or institutions; and
- To be responsible for or complicit in, or to have engaged in, the receipt or use for commercial or competitive advantage or private financial gain, or by a commercial entity, outside the United States of trade secrets misappropriated through cyber-enabled means, knowing they have been misappropriated, where the misappropriation of such trade secrets is reasonably likely to result in, or has materially contributed to, a significant threat to the national security, foreign policy, or economy of the United States;

- To have materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services in support of, certain activities described above or any person whose property and interests in property are blocked pursuant to E.O. 13694, as amended;
- To be owned or controlled by, or to have acted or purported to act for or on behalf of, directly or indirectly, any person whose property and interests in property are blocked pursuant to E.O. 13694, as amended; or
- To have attempted to engage in any of the activities described in E.O. 13694, as amended.

On December 31, 2015, OFAC issued an abbreviated set of regulations to implement E.O. 13694. See the Cyber-Related Sanctions Regulations, [31 C.F.R. part 578](#) (the “Regulations”), for details. OFAC intends to supplement the Regulations with a more comprehensive set of regulations, which may include additional interpretive and definitional guidance and additional general licenses and statements of licensing policy.

The names of individuals and entities listed in the Annex to E.O. 13694, as amended, or designated pursuant to E.O. 13694, as amended, and whose property and interests in property are therefore blocked, are published in the *Federal Register* and incorporated into OFAC’s Specially Designated Nationals and Blocked Persons List (SDN List) with the identifier “[CYBER].” The SDN List and Treasury’s other sanctions lists are available on OFAC’s website at www.treasury.gov/sdn.

This fact sheet is a broad summary of the sanctions as of the date of publication. For an updated list of authorities and sanctions please refer to the Cyber-related Sanctions page on OFAC’s website at: www.treasury.gov/resource-center/sanctions/Programs/pages/cyber.aspx.

III. PROHIBITED TRANSACTIONS

Unless otherwise authorized or exempt, transactions by U.S. persons, or in or involving the United States, are prohibited if they involve transferring, paying, exporting, withdrawing, or otherwise dealing in the property or interests in property of an entity or individual listed on the SDN List. The property and interests in property of an entity that is 50 percent or more directly or indirectly owned, whether individually or in the aggregate, by one or more blocked persons are also blocked, regardless of whether the entity itself is listed or identified on the SDN List. For details please see: www.treasury.gov/resource-center/sanctions/Documents/licensing_guidance.pdf.

IV. AUTHORIZED TRANSACTIONS

GENERAL LICENSES

OFAC may authorize certain types or categories of activities and transactions that would otherwise be prohibited with respect to cyber-related sanctions by issuing a general license. General licenses may be published in the Regulations or on OFAC’s website. For example:

- Section 578.506 of the Regulations authorizes the provision of certain legal services to or on behalf of persons whose property and interests in property are blocked pursuant to section 578.201 of the Regulations, provided that the receipt of payment of professional fees and reimbursement of incurred expenses must be specifically licensed, authorized pursuant to section 578.507 of the Regulations, which authorizes certain payments for legal services from funds originating outside the United States, or otherwise authorized.
- On February 2, 2017, OFAC issued [General License No. 1](#) authorizing certain transactions with Russia’s Federal Security Service (a.k.a. FSB) that are necessary and ordinarily incident to requesting, utilizing, paying for, or dealing in certain licenses and authorizations for the importation, distribution, or use of certain information technology products in the Russian Federation, subject to certain limitations described in the General License, as well as transactions necessary and ordinarily incident to compliance with rules and regulations administered by, and certain actions or investigations involving, the FSB.

For a current list of all general licenses relating to the cyber-related sanctions program, please see subpart E of the Regulations and visit: www.treasury.gov/resource-center/sanctions/Programs/Pages/cyber.aspx.

SPECIFIC LICENSES

On a case-by-case basis, OFAC considers applications for specific licenses to authorize transactions that are neither exempt nor authorized by a general license. Requests for a specific license must be submitted to OFAC's Licensing Division. Specific license requests may be submitted using either of the following methods:

- Online: www.treasury.gov/resource-center/sanctions/Pages/licensing.aspx; or
- Mail: Assistant Director for Licensing, Office of Foreign Assets Control, U.S. Department of the Treasury, 1500 Pennsylvania Avenue, N.W., Freedman's Bank Building, Washington, DC 20220.

V. ENFORCEMENT & PENALTIES

OFAC uses the Economic Sanctions Enforcement Guidelines, 31 C.F.R. part 501, app. A (the "Guidelines"), in determining the appropriate enforcement response to apparent violations of U.S. economic sanctions programs that OFAC administers and enforces. For more information about OFAC's enforcement process, please review the Guidelines [here](#).

Civil monetary penalties of up to the greater of \$250,000 (\$289,238 as of January 15, 2017 for violations occurring after November 2, 2015) or twice the amount of the underlying transaction may be imposed administratively against any person who violates, attempts to violate, conspires to violate, or causes a violation of any license, order, regulation or prohibition issued under IEEPA.

Upon conviction, criminal penalties of up to \$1,000,000, imprisonment for up to 20 years, or both, may be imposed on any person who willfully commits, willfully attempts to commit, or willfully conspires to commit, or aids or abets in the commission of a violation of any license, order, regulation, or prohibition issued under IEEPA.

This document is explanatory only and does not have the force of law. E.O. 13694, as amended and the Regulations contain the relevant legally binding provisions governing the sanctions. This document does not supplement or modify the Executive orders, the Regulations, or any other applicable laws.

GENERAL SANCTIONS INFORMATION

OFAC administers a number of U.S. economic sanctions programs. OFAC sanctions programs can range from being comprehensive in nature, such as a program that blocks the entire government of a country and includes broad geographically-based trade restrictions, to being fairly limited, such as a program that targets only specific individuals and entities. Some programs both target particular individuals and entities and prohibit types of transactions. It is therefore important to review the details of any given sanctions program to understand its scope. It is also important to note that although a program may be targeted, the prohibitions in such programs on dealings with individuals and entities whose property and interests in property are blocked are very broad, and they apply regardless of where the targeted person is located. The names of individuals and entities that are designated or identified as blocked by OFAC are incorporated into OFAC's SDN List. Note, however, that the SDN List is not a comprehensive list of all entities and individuals whose property and interests in property are blocked. For example, the property and interests in property of an entity that is 50 percent or more directly or indirectly owned, whether individually or in the aggregate, by one or more blocked persons are also blocked, regardless of whether the entity itself is listed on the SDN List. Note also that, in certain programs, blocking of the property and interests in property of a Government extends to entities owned or controlled by that Government, whether or not they are identified on the SDN List.

Please note that OFAC maintains other sanctions lists that may have different prohibitions associated with them. See the "[Sanctions Programs and Country Information](#)" page for information on specific programs and other Treasury sanctions lists at: www.treasury.gov/resource-center/sanctions/SDN-List/Pages/Other-OFAC-Sanctions-Lists.aspx. Because OFAC's programs are constantly changing, it is very important to check OFAC's website on a regular basis. You may also wish to sign up for updates via OFAC's [Email Notification System](#) to receive notifications regarding

changes to OFAC's sanctions programs. For additional information about these programs or about sanctions involving cyber-related matters, please contact:

OFFICE OF FOREIGN ASSETS CONTROL

U.S. Department of the Treasury
1500 Pennsylvania Avenue, N.W.

Freedman's Bank Building

Washington, DC 20220

www.treasury.gov/ofac

(202) 622-2490



DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments¹

Date: October 1, 2020

The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) is issuing this advisory to highlight the sanctions risks associated with ransomware payments related to malicious cyber-enabled activities. 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. This advisory describes these sanctions risks and provides information for contacting relevant U.S. government agencies, including OFAC, if there is a reason to believe the cyber actor demanding ransomware payment may be sanctioned or otherwise have a sanctions nexus.²

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 ransomware payment, usually through digital 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's 2018 and 2019 Internet Crime Reports, there was a 37 percent annual increase in reported ransomware cases and a 147 percent annual increase in associated losses from 2018 to 2019.³ While ransomware attacks are carried out against large corporations, many ransomware attacks also target small- and medium-sized

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 particular requirements under applicable law. Please see the legally binding provisions cited for relevant legal authorities.

² 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, Criminal Division, Computer Crime and Intellectual Property Section, Cybersecurity Unit, *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>.

³ Compare Federal Bureau of Investigation, Internet Crime Complaint Center, *2018 Internet Crime Report*, at 19, 20, available at https://pdf.ic3.gov/2018_IC3Report.pdf, with Federal Bureau of Investigation, Internet Crime Complaint Center, *2019 Internet Crime Report*, available at https://pdf.ic3.gov/2019_IC3Report.pdf.

businesses, local government agencies, hospitals, and school districts, which may be more vulnerable as they may have fewer resources to invest in cyber protection.

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.⁴ OFAC designated the developer of Cryptolocker, Evgeniy Mikhailovich Bogachev, in December 2016.⁵

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 digital currency addresses used to funnel SamSam ransomware proceeds.⁶

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 sub-groups, Bluenoroff and Andariel, in September 2019.⁷

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.⁸

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.

⁴ Press Release, U.S. Dept. of Justice, U.S. Leads Multi-National Action Against “GameOver Zeus” Botnet and “Cryptolocker” Ransomware, Charges Botnet Administrator (June 2, 2014), available at <https://www.justice.gov/opa/pr/us-leads-multi-national-action-against-gameover-zeus-botnet-and-cryptolocker-ransomware>.

⁵ Press Release, U.S. Dept. of the Treasury, Treasury Sanctions Two Individuals for Malicious Cyber-Enabled Activities (Dec. 29, 2016), available at <https://www.treasury.gov/press-center/press-releases/Pages/jl0693.aspx>.

⁶ Press Release, U.S. Dept. of the Treasury, Treasury Designates Iran-Based Financial Facilitators of Malicious Cyber Activity and for the First Time Identifies Associated Digital Currency Addresses (Nov. 28, 2018), available at <https://home.treasury.gov/news/press-releases/sm556>.

⁷ Press Release, U.S. Dept. of the Treasury, Treasury Sanctions North Korean State-Sponsored Malicious Cyber Groups (Sept. 13, 2019), available at <https://home.treasury.gov/news/press-releases/sm774>.

⁸ Press Release, U.S. Dept. of the Treasury, Treasury Sanctions Evil Corp, the Russia-Based Cybercriminal Group Behind Dridex Malware (Dec. 5, 2019), available at <https://home.treasury.gov/news/press-releases/sm845>.

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. Ransomware payments may also embolden cyber actors to engage in future attacks. In addition, paying a ransom to cyber actors does not guarantee that the victim will regain access to its stolen data.

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),⁹ 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 transactions by a non-U.S. person which causes a U.S. person to violate any IEEPA-based sanctions, is also prohibited. U.S. persons, wherever located, are also generally prohibited from facilitating actions of non-U.S. persons, which 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 it did not know or have reason to know it was engaging in a transaction with a person that is prohibited under sanctions laws and regulations administered by OFAC.

OFAC’s Economic Sanctions Enforcement Guidelines (Enforcement Guidelines)¹⁰ 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. Under the Enforcement Guidelines, in the event of an apparent violation of U.S. sanctions laws or regulations, the existence, nature, and adequacy of a sanctions compliance program is a factor that OFAC may consider when determining an appropriate enforcement response (including the amount of civil monetary penalty, if any).

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.¹¹ 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

⁹ 50 U.S.C. §§ 4301–41; 50 U.S.C. §§ 1701–06.

¹⁰ 31 C.F.R. part 501, appx. A.

¹¹ 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.

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.¹²

Under OFAC's Enforcement Guidelines, OFAC will also consider a company's self-initiated, timely, and complete report of a ransomware attack to law enforcement to be a significant mitigating factor in determining an appropriate enforcement outcome if the situation is later determined to have a sanctions nexus. OFAC will also consider a company's full and timely cooperation with law enforcement both during and after a ransomware attack to be a significant mitigating factor when evaluating a possible enforcement outcome.

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 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 encourages victims and those involved with addressing ransomware attacks to contact OFAC immediately if they believe a request for a ransomware payment may involve a sanctions nexus. Victims should also contact the U.S. Department of the Treasury's Office of Cybersecurity and Critical Infrastructure Protection if an attack involves a U.S. financial institution or may cause significant disruption to a firm's ability to perform critical financial services.

- 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
- Financial Crimes Enforcement Network (FinCEN)
 - FinCEN Regulatory Support Section: frc@fincen.gov

¹² See FinCEN Guidance, FIN-2020-A00X, "[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.

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

- Federal Bureau of Investigation Cyber Task Force
 - <https://www.ic3.gov/default.aspx>; www.fbi.gov/contact-us/field
- U.S. Secret Service Cyber Fraud Task Force
 - www.secretservice.gov/investigation/#field
- Cybersecurity and Infrastructure Security Agency
 - <https://us-cert.cisa.gov/forms/report>
- Homeland Security Investigations Field Office
 - <https://www.ice.gov/contact/hsi>

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.



FinCEN ADVISORY

FIN-2020-A006

October 1, 2020

Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments

Detecting and reporting ransomware payments are vital to prevent and deter cybercriminals from deploying malicious software to extort individuals and businesses and hold ransomware attackers accountable for their crimes.

This Advisory should be shared with:

- Chief Executive Officers
- Chief Operating Officers
- Chief Compliance Officers
- Chief Risk Officers
- Chief Information Officers
- AML/BSA Departments
- Legal Departments
- Cyber and Security Departments
- Customer Service Agents
- Bank Tellers

SAR Filing Request:

FinCEN requests financial institutions reference this advisory in SAR field 2 (Filing Institution Note to FinCEN) and the narrative by including the following key term: “CYBER FIN-2020-A006” and select SAR field 42 (Cyber Event). Additional guidance on filing SARs appears near the end of this advisory.

Introduction

The Financial Crimes Enforcement Network (FinCEN) is issuing this advisory to alert financial institutions to predominant trends, typologies, and potential indicators of ransomware and associated money laundering activities. This advisory provides information on: (1) the role of financial intermediaries in the processing of ransomware payments; (2) trends and typologies of ransomware and associated payments; (3) ransomware-related [financial red flag indicators](#); and (4) reporting and sharing information related to ransomware attacks.

The information contained in this advisory is derived from FinCEN’s analysis of cyber- and ransomware-related Bank Secrecy Act (BSA) data, open source reporting, and law enforcement partners.

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 (IT) systems to extort ransom payments from victims in exchange for decrypting the information and restoring victims’ access to their systems or data.¹ In some cases, in addition to the attack, the perpetrators threaten to publish sensitive files belonging to the victims, which can be individuals or business entities

1. Both extortion and computer fraud and abuse are specified unlawful activities and predicate offenses to money laundering. See 18 USC § 1956(c)(7).

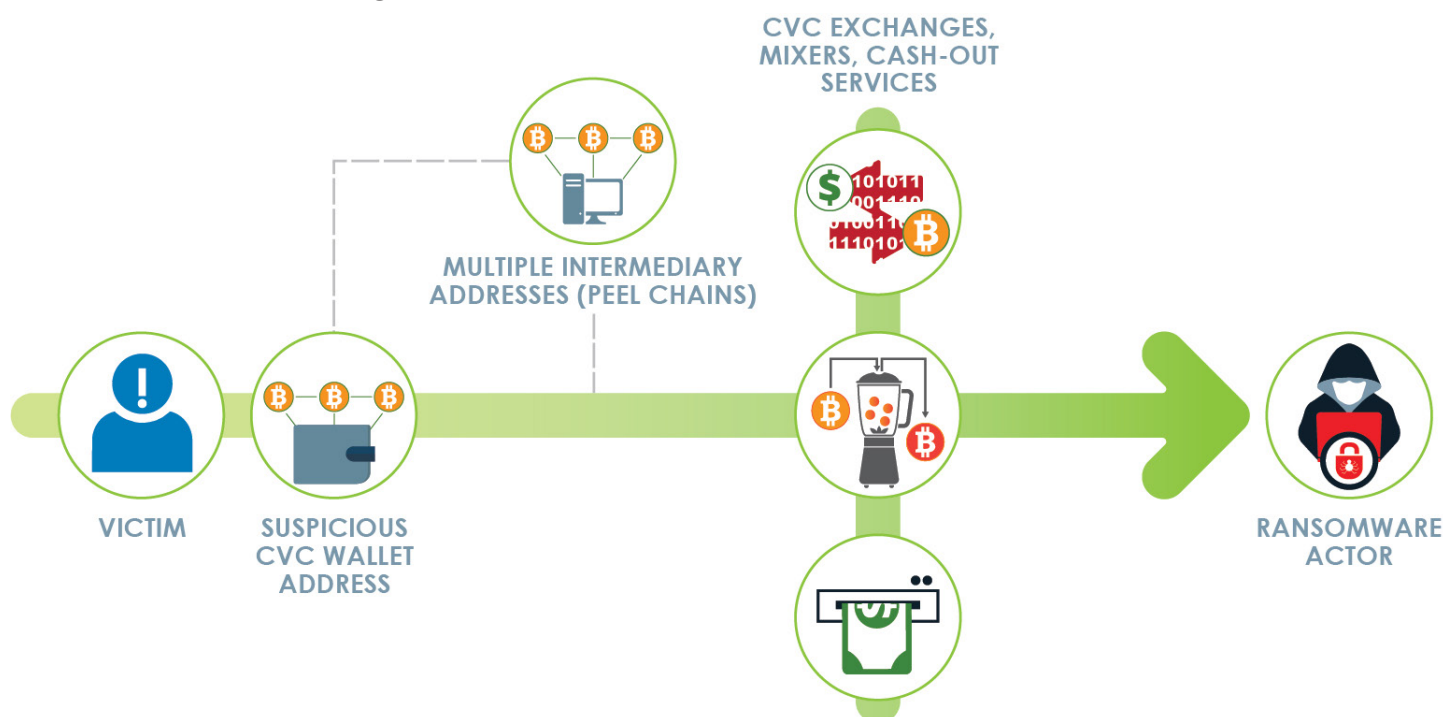
(including financial institutions). The consequences of a ransomware attack can be severe and far-reaching — with losses of sensitive, proprietary, and critical information and/or loss of business functionality.

The Role of Financial Intermediaries in Facilitating Ransomware Payments

Ransomware attacks are a growing concern for the financial sector because of the critical role financial institutions play in the collection of ransom payments. Processing ransomware payments is typically a multi-step process that involves at least one depository institution and one or more money services business (MSB). Many ransomware schemes involve convertible virtual currency (CVC), the preferred payment method of ransomware perpetrators. Following the delivery of the ransom demand, a ransomware victim will typically transmit funds via wire transfer, automated clearinghouse, or credit card payment to a CVC exchange to purchase the type and amount of CVC specified by the ransomware perpetrator. Next, the victim will send the CVC, often from a wallet hosted² at the exchange, to the perpetrator's designated account or CVC address. The perpetrator then launders the funds through various means, including mixers and tumblers³ to convert funds into other CVCs, smurfing⁴ transactions across many accounts and exchanges, and/or moving the CVC to foreign-located exchanges and peer-to-peer (P2P) exchangers⁵ in jurisdictions with weak anti-money laundering and countering financing of terrorism (AML/CFT) controls.

2. "Hosted wallets" are CVC wallets where the CVC exchange receives, stores, and transmits the CVCs on behalf of their accountholders. See FinCEN Guidance, [FIN-2019-G001](#), "Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies," (May 9, 2019).
3. Mixing or tumbling involves the use of mechanisms to break the connection between an address sending CVC and the addresses receiving CVC.
4. Smurfing refers to a layering technique in money laundering that involves breaking total amounts of funds into smaller amounts to move through multiple accounts before arriving at the ultimate beneficiary.
5. P2P exchangers are individuals or entities offering to exchange fiat currencies for virtual currencies or one virtual currency for another virtual currency. P2P exchangers usually operate informally, typically advertising and marketing their services through online classified advertisements or fora, social media, and by word of mouth. See FinCEN Advisory, [FIN-2019-A003](#), "Advisory on Illicit Activity Involving Convertible Virtual Currency," (May 9, 2019).

Figure 1. Movement of CVC in Ransomware Attacks



Involvement of Digital Forensics and Incident Response and Cyber Insurance Companies in Ransomware Payments

The prevalence of ransomware attacks has led to the creation of companies that provide protection and mitigation services to victims of ransomware attacks. Among these entities are digital forensics and incident response (DFIR) companies and cyber insurance companies (CICs). Some DFIR companies and CICs, as well as some MSBs that offer CVCs, facilitate ransomware payments to cybercriminals, often by directly receiving customers' fiat funds, exchanging them for CVC, and then transferring the CVC to criminal-controlled accounts. Depending on the particular facts and circumstances, this activity could constitute money transmission. Entities engaged in money services business activities (such as money transmission) are required to register as an MSB with FinCEN, and are subject to BSA obligations, including filing suspicious activity reports (SARs).⁶ Persons involved in ransomware payments must also be aware of any Office of Foreign Assets Control (OFAC)-related obligations that may arise from that activity. Today, OFAC issued an [advisory](#) highlighting the sanctions risks associated with facilitating ransomware payments on behalf of victims targeted by malicious cyber-enabled activities.

6. See generally 31 C.F.R. Part 1022 and 31 CFR § 1010.100(ff).

Trends and Typologies of Ransomware and Associated Payments

The severity and sophistication of ransomware attacks continue to rise⁷ across various sectors, particularly across governmental entities, and financial, educational, and healthcare institutions.⁸ Ransomware attacks on small municipalities and healthcare organizations have increased, likely due to the victims' weaker cybersecurity controls, such as inadequate system backups and ineffective incident response capabilities.⁹

Cybercriminals using ransomware often resort to common tactics, such as wide-scale phishing and targeted spear-phishing campaigns that induce victims to download a malicious file or go to a malicious site, exploit remote desktop protocol endpoints and software vulnerabilities, or deploy "drive-by" malware attacks that host malicious code on legitimate websites. Proactive prevention through effective cyber hygiene, cybersecurity controls, and business continuity resiliency is often the best defense against ransomware.¹⁰

Increasing Sophistication of Ransomware Operations

Big Game Hunting Schemes: Ransomware actors are increasingly engaging in selective targeting of larger enterprises to demand bigger payouts – commonly referred to as "big game hunting."¹¹

Ransomware Criminals Forming Partnerships and Sharing Resources: Many cybercriminals are sharing resources to enhance the effectiveness of ransomware attacks, such as ransomware exploit kits that come with ready-made malicious codes and tools. These kits can be purchased, although they are also offered free of charge. Some ransomware groups are also forming partnerships to share advice, code, trends, techniques, and illegally-obtained information over shared platforms.

"Double Extortion" Schemes: Ransomware criminals are increasingly engaging in "double extortion schemes," which involve removing sensitive data from the targeted networks and encrypting the system files and demanding ransom. The criminals then threaten to publish or sell the stolen data if the victim fails to pay the ransom.




7. The Federal Bureau of Investigation (FBI) Internet Crime Complaint Center (IC3) received 37% more reports of ransomware incidents in 2019 than in 2018, with a 46% increase in associated financial losses. BSA reporting shows a stark increase in financial losses per ransomware incident, with the average dollar amount in financial institution SARs on ransomware increasing approximately \$87,000 from 2018 to 2019 (\$417,000 to \$504,000) and \$280,000 from 2019 to thus far in 2020 (\$504,000 to \$783,000). See FBI IC3, "[2019 Internet Crime Report](#)," (2019); and FBI IC3, "[2018 Internet Crime Report](#)," (2018).
8. See FinCEN Advisory, [FIN-2020-A005](#), "Advisory on Cybercrime and Cyber-Enabled Crime Exploiting the Coronavirus Disease 2019 (COVID-19) Pandemic," (July 30, 2020).
9. Multi-State Information Sharing and Analysis Center (MS-ISAC), "[Security Primer – Ransomware](#)," (May 2020).
10. For more information about ransomware risk, see Federal Financial Institutions Examination Council (FFIEC), Press Release, "[FFIEC Releases Statement on Cyber Attacks Involving Extortion](#)," (November 3, 2015); Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA), "[Security Tip \(ST19-001\): Protecting against Ransomware](#)," (April 11, 2019); and DHS CISA, MS-ISAC, National Governors Association (NGA), and National Association of State Chief Information Officers (NASCIO), Joint Alert, "[CISA, MS-ISAC, NGA & NASCIO Recommend Immediate Action to Safeguard against Ransomware](#)," (July 29, 2019).
11. See FBI Public Service Announcement, [Alert No. I-100219-PSA](#), "High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations," (October 2, 2019).

Use of Anonymity-Enhanced Cryptocurrencies (AECs): Cybercriminals usually require ransomware payments to be denominated in CVCs, most commonly in bitcoin (see Figure 1). However, they are also increasingly requiring or incentivizing victims to pay in AECs that reduce the transparency of CVC financial flows, including ransomware payments, through anonymizing features, such as mixing and cryptographic enhancements.¹² Some ransomware operators have even offered discounted rates to victims who pay their ransoms in AECs.

Use of “Fileless” Ransomware: Fileless ransomware is a more sophisticated tool that can be challenging to detect because the malicious code is written into the computer’s memory rather than into a file on a hard drive, which allows attackers to circumvent off-the-shelf antivirus and malware defenses.¹³

Financial Red Flag Indicators of Ransomware and Associated Payments

FinCEN has identified the following financial red flag indicators of ransomware-related illicit activity to assist financial institutions in detecting, preventing, and reporting suspicious transactions associated with ransomware attacks. As no single financial red flag indicator is indicative of illicit or suspicious activity, financial institutions should consider the relevant facts and circumstances of each transaction, in keeping with their risk-based approach to compliance.¹⁴








-  1 IT enterprise activity is connected to cyber indicators that have been associated with possible ransomware activity or cyber threat actors known to perpetrate ransomware schemes. Malicious cyber activity may be evident in system log files, network traffic, or file information.¹⁵
-  2 When opening a new account or during other interactions with the financial institution, a customer provides information that a payment is in response to a ransomware incident.
-  3 A customer’s CVC address, or an address with which a customer conducts transactions, appears on open sources, or commercial or government analyses have linked those addresses to ransomware strains, payments, or related activity.

12. See FinCEN Advisory, [FIN-2019-A003](#), “Advisory on Illicit Activity Involving Convertible Virtual Currency,” (May 9, 2019).

13. The MS-ISAC observed a 153% increase of reported instances of ransomware targeting state, local, tribal, and territorial governments from 2018 to 2019. See MS-ISAC, “[Security Primer – Ransomware](#),” (May 2020).

14. For more information about red flags of illicit CVC use, see FinCEN Advisory, [FIN-2019-A003](#), “Advisory on Illicit Activity Involving Convertible Virtual Currency,” (May 9, 2019).

15. For example cyber indicators of compromise on specific ransomware threats, see DHS CISA Technical Alerts, “[Ransomware Alerts](#).” For other cyber indicator resources, see also FinCEN’s Cyber Indicator Lists (CILs), shared through the FinCEN Secure Information Sharing System; the U.S. Department of the Treasury’s Office of Cybersecurity and Critical Infrastructure Protection’s CILs and circulars, available upon request; and DHS CISA’s [cyber analytic products and services](#), including a comprehensive list of COVID-19-related indicators of compromise in [CSV](#) or [STIX-formatted XML](#) formats, the [Cyber Information Sharing and Collaboration Program \(CISCP\)](#), and the [Automated Indicator Sharing \(AIS\) program](#). Public-private and industry partnerships, such as the [Financial Services Information Sharing and Analysis Center](#), and open source and commercial cyber threat feeds can also be useful resources.

-  4 A transaction occurs between an organization, especially an organization from a sector at high risk for targeting by ransomware (e.g., government, financial, educational, healthcare), and a DFIR or CIC, especially one known to facilitate ransomware payments.
-  5 A DFIR or CIC customer receives funds from a customer company and shortly after receipt of funds sends equivalent amounts to a CVC exchange.
-  6 A customer shows limited knowledge of CVC during onboarding or via other interactions with the financial institution, yet inquires about or purchases CVC (particularly if in a large amount or rush requests), which may indicate the customer is a victim of ransomware.
-  7 A DFIR, CIC, or other company that has no or limited history of CVC transactions sends a large CVC transaction, particularly if outside a company's normal business practices.
-  8 A customer that has not identified itself to the CVC exchanger, or registered with FinCEN as a money transmitter, appears to be using the liquidity provided by the exchange to execute large numbers of offsetting transactions between various CVCs, which may indicate that the customer is acting as an unregistered MSB.
-  9 A customer uses a CVC exchanger or foreign-located MSB in a high-risk jurisdiction lacking, or known to have inadequate, AML/CFT regulations for CVC entities.
-  10 A customer initiates multiple rapid trades between multiple CVCs, especially AECs, with no apparent related purpose, which may be indicative of attempts to break the chain of custody on the respective blockchains or further obfuscate the transaction.

Reminder of Regulatory Obligations for U.S. Financial Institutions Regarding Suspicious Activity Reporting Involving Ransomware and USA PATRIOT ACT Section 314(b) Information Sharing Authority

Suspicious Activity Reporting

Financial institutions can play an important role in protecting the U.S. financial system from ransomware threats through compliance with their BSA obligations. Financial institutions should determine if filing a SAR is required or appropriate when dealing with an incident of ransomware conducted *by, at, or through* the financial institution, including ransom payments made by financial institutions that are victims of ransomware. As a reminder, a financial institution is required to file a SAR if it knows, suspects, or has reason to suspect a transaction conducted or attempted by, at, or through the financial institution involves or aggregates to \$5,000 (or, with one exception, \$2,000 for MSBs)¹⁶ or more in funds or other assets and involves

16. See 31 C.F.R. §§ 1020.320, 1021.320, 1022.320, 1023.320, 1024.320, 1025.320, 1026.320, 1029.320, and 1030.20. The monetary threshold for filing money services businesses SARs is, with one exception, set at or above \$2,000. See also 31 C.F.R. § 1022.320(a)(2).

funds derived from illegal activity, or attempts to disguise funds derived from illegal activity; is designed to evade regulations promulgated under the BSA; lacks a business or apparent lawful purpose; or involves the use of the financial institution to facilitate criminal activity. Reportable activity can involve transactions, including payments made by financial institutions, related to criminal activity like extortion and unauthorized electronic intrusions that damage, disable, or otherwise affect critical systems. SAR obligations apply to both *attempted and successful* transactions, including both attempted and successful initiated extortion transactions.¹⁷

Financial institutions are required to file complete and accurate reports that incorporate *all relevant information available*, including cyber-related information. When filing a SAR regarding suspicious transactions that involve cyber events (including ransomware), financial institutions should provide all pertinent available information on the event and associated with the suspicious activity, including cyber-related information and technical indicators, in the SAR form and narrative. When filing is not required, institutions may file a SAR voluntarily to aid law enforcement in protecting the financial sector. Valuable cyber indicators for law enforcement investigations for ransomware can include relevant email addresses, Internet Protocol (IP) addresses with their respective timestamps, login information with location and timestamps, virtual currency wallet addresses, mobile device information (such as device International Mobile Equipment Identity (IMEI) numbers), malware hashes, malicious domains, and descriptions and timing of suspicious electronic communications.

When a financial institution files a SAR, it is required to maintain a copy of the SAR and the original or business record equivalent of any supporting documentation for a period of five years from the date of filing the SAR.¹⁸ Financial institutions must provide any requested SAR and all documentation supporting the filing of a SAR upon request by FinCEN or an appropriate law enforcement or supervisory agency.¹⁹ When requested to provide supporting documentation, financial institutions should take special care to verify that a requestor of information is, in fact, a representative of FinCEN or an appropriate law enforcement or supervisory agency. A financial institution should incorporate procedures for such verification into its BSA compliance or anti-money laundering program. These procedures may include, for example, independent employment verification with the requestor's field office or face-to-face review of the requestor's credentials.²⁰

17. FinCEN assesses that ransomware-related activity is under-reported.

18. See 31 C.F.R. §§ 1020.320(d), 1021.320(d), 1022.320(c), 1023.320(d), 1024.320(c), 1025.320(d), and 1026.320(d).

19. *Id.* See also FinCEN Guidance, [FIN-2007-G003](#), "Suspicious Activity Report Supporting Documentation," (June 13, 2007).

20. FinCEN Guidance, [FIN-2007-G003](#), "Suspicious Activity Report Supporting Documentation," (June 13, 2007).

SAR Filing Instructions

FinCEN requests that financial institutions reference this advisory by including the key term:

“CYBER-FIN-2020-A006”

in SAR field 2 (Filing Institution Note to FinCEN) and the narrative to indicate a connection between the suspicious activity being reported and ransomware-related activity.

Financial institutions should also select SAR field 42 (Cyber event) as the associated suspicious activity type, as well as select SAR field 42z (Cyber event - Other) while including “ransomware” as keywords in SAR field 42z, to indicate a connection between the suspicious activity being reported and possible ransomware activity. Additionally, financial institutions should include any relevant technical cyber indicators related to the ransomware activity and associated transactions within the available structured cyber event indicator SAR fields 44(a)-(j), (z).

Information Sharing

Information sharing among financial institutions is critical to identifying, reporting, and preventing evolving ransomware schemes. Financial institutions sharing information under the safe harbor authorized by section 314(b) of the USA PATRIOT Act are reminded that they may share information relating to transactions that the institution suspects may involve the proceeds of one or more specified unlawful activities (“SUAs”) and such an institution will still remain protected from civil liability under the section 314(b) safe harbor. The SUAs listed in 18 U.S.C. §§ 1956 and 1957 include an array of fraudulent and other criminal activities, including extortion and computer fraud and abuse. FinCEN strongly encourages information sharing via section 314(b) where financial institutions suspect that a transaction may involve terrorist financing or money laundering, including one or more SUAs.²¹

For Further Information

Questions or comments regarding the contents of this advisory should be addressed to the FinCEN Regulatory Support Section at frc@fincen.gov.

The mission of the Financial Crimes Enforcement Network is to safeguard the financial system from illicit use, combat money laundering and its related crimes including terrorism, and promote national security through the strategic use of financial authorities and the collection, analysis, and dissemination of financial intelligence.

21. For further guidance related to the 314(b) Program, see FinCEN [Fact Sheet](#), “Section 314(b)” (November 2016) and FinCEN Guidance, [FIN-2009-G002](#), “Guidance on the Scope of Permissible Information Sharing Covered by Section 314(b) Safe Harbor of the USA PATRIOT Act,” (June 16, 2009).

July 6, 2021 | 4:40 pm

COVID-19 Updates

The COVID-19 vaccine is here. It is safe, effective and free. Walk in to get vaccinated at sites across the state. Continue to mask up and stay distant where directed.

GET THE FACTS >

Department of Financial Services

Insurance Circular Letter No. 2 (2021)

February 4, 2021

TO:	All Authorized Property/Casualty Insurers
RE:	Cyber Insurance Risk Framework

REGULATORY REFERENCE: 23 NYCRR 500

Introduction

As cybercrime becomes more common and costly, cyber risk continues to increase for all organizations. The COVID-19 pandemic has shifted more of our work and lives online, and this shift has introduced new vulnerabilities that cybercriminals are aggressively exploiting.^[1] From the rise of ransomware to the recently revealed SolarWinds-based cyber-espionage campaign, it is clear that cybersecurity is now critically important to almost every aspect of modern life – from consumer protection to national security. This is why DFS has led by promulgating the nation's first cybersecurity regulation for financial services in 2017 and creating its Cybersecurity Division in 2019.

Cyber insurance plays a key role in managing and reducing cyber risk. This is a relatively new area of insurance for most insurers, but one that has grown rapidly. In 2019 the U.S. cyber insurance market was \$3.15 billion.^[2] It is estimated that by 2025, it will be over \$20 billion.^[3] And these numbers understate insurance coverage of cyber risk, as many insurance claims

Industry Guidance

under non-cyber insurance policies. As the
s to facilitate the continued growth of a sustainable

and sound cyber insurance market.

A robust cyber insurance market that effectively prices cyber risk will also improve cybersecurity. By identifying and pricing risk created by gaps in cybersecurity, cyber insurance can create a financial incentive to fill those gaps to reduce premiums.^[4] By driving improved cybersecurity and cyber risk management, cyber insurance can also benefit consumers who entrust their sensitive data to these organizations.

To foster the growth of a robust cyber insurance market that maintains the financial stability of insurers and protects insureds, we have created a Cyber Insurance Risk Framework that outlines best practices for managing cyber insurance risk (the “Framework”). The Framework is based on our extensive consultation with industry, cybersecurity experts, and other stakeholders. The Framework applies to all authorized property/casualty insurers that write cyber insurance. However, property/casualty insurers that do not write cyber insurance should still evaluate their exposure to “silent risk” and take appropriate steps to reduce that exposure.

The Risks for Insurers

As cyber risk has increased, so too has risk in underwriting cyber insurance. The damage done by many types of cybercrime – such as business email compromises – continues to rise. But the biggest driver is an increase in the frequency and cost of ransomware attacks. A 2020 survey by DFS revealed that from early 2018 to late 2019, the number of insurance claims arising from ransomware increased by 180%, and the average cost of a ransomware claim rose by 150%. Moreover, the number of ransomware attacks reported to DFS almost doubled in 2020 from the previous year.^[5] Costs continued to rise in 2020 as ransomware attacks increased in frequency and scale.^[6] The global cost of ransomware was approximately \$20 billion in 2020.^[7] The cyber insurance industry has reported that escalating costs are creating pressure to increase rates and tighten underwriting standards for cyber insurance.

DFS recommends against making ransom payments. Ransom payments fuel the vicious cycle of ransomware, as cybercriminals use them to fund ever more frequent and sophisticated ransomware attacks. An October 2020 guidance by the Office of Foreign Assets Control (“OFAC”) stressed the national security risk posed by ransom payments, and stated that intermediaries – including insurers – can be liable for ransom payments made to sanctioned entities.^[8] Given the problem of identifying the attacker at the time of a ransomware incident, insurers and their policyholders risk violating OFAC sanctions when paying a ransom. Similarly, the FBI warns against paying a ransom because it fails to guarantee that an organization will

Industry Guidance

a won't be released publicly, and also because get other organizations. In 2020, data extortion

became a common feature of ransomware attacks, but experts have noted that in many cases even when victims paid, their data was subsequently leaked.^[9]

Many insurers still have work to do to develop a rigorous and data driven approach to cyber risk, and experts have expressed concerns that insurers are not yet able to accurately measure cyber risk.^[10] The decision to offer and price cyber insurance for specific organizations should be based on a careful assessment of that organization's risk. Cyber risk is driven in large part by the caliber of an organization's cybersecurity program, and so can vary considerably from one organization to the next. Insurers that don't effectively measure the risk of their insureds also risk insuring organizations that use cyber insurance as a substitute for improving cybersecurity, and pass the cost of cyber incidents on to the insurer. Without an effective ability to measure risk, cyber insurance can therefore have the perverse effect of increasing cyber risk – risk that will be borne by the insurer.

Managing this growing cyber risk is an urgent challenge for insurers. In addition to overall rising costs, insurers must account for the systemic risk that occurs when a widespread cyber incident damages many insureds at the same time, potentially swamping insurers with massive losses. This systemic risk is illustrated by the massive supply chain compromise in SolarWinds' Orion enterprise network management software.^[11] Orion was widely used by critical infrastructure entities, private sector organizations, service providers, and government agencies. As a result of the compromise, thousands of organizations had malware backdoors installed in their networks. We have been assessing the impact of this compromise and appreciate the engagement of industry in this process.^[12] Although this cyber campaign appears to have been focused on espionage and not destructive attacks, given the number of impacted organizations the total remediation costs are likely to be substantial.

Moreover, insurers often incur losses from cyber incidents in insurance policies that do not explicitly grant or exclude cyber coverage – so-called “non-affirmative” or “silent” risk. Because silent risk can reside in many different types of policies, even insurers that write little or no cyber insurance need to measure and manage silent risk in their non-cyber insurance policies. While the industry has taken steps to address silent risk in recent years, it remains a significant problem for many insurers. According to a global survey in the second quarter of 2020, 65% of underwriters were concerned about cyber coverage exposure in property/casualty policies that do not explicitly cover cyber risks.^[13]

Industry Guidance

risk – are exemplified by the 2017 NotPetya Russian government caused damage across the globe. The incident led to \$3 billion in insurance claims, of which \$2.7 billion were made under property/casualty policies that were silent about cyber risks.^[14]

The Framework is a result of our ongoing dialogue with the insurance industry and experts on cyber insurance. Over the past year, we have had dozens of meetings with insurers, insurance producers, cyber experts, and insurance regulators across the U.S. and Europe. In July 2020, we hosted a cyber insurance roundtable with representatives from five global insurance groups. Also in 2020, we collected survey data from 49 insurers on cyber insurance and ransomware. We continue to welcome input from industry and other interested parties on challenges facing the cyber insurance market.

Conclusion

Insurers play a critical role in mitigating and reducing the risks of cybercrime. We commend the progress many insurers have made in managing their cyber insurance risk to date and look forward to continuing to work with the industry to address challenges in the cyber insurance market.

Please direct any questions regarding this Circular Letter to CyberInsurance@dfs.ny.gov.

Sincerely,

Linda A. Lacewell

Superintendent

Cyber Insurance Risk Framework

All authorized property/casualty insurers that write cyber insurance should employ the practices identified below to sustainably and effectively manage their cyber insurance risk.^[15] Based on our engagement with industry and experts, certain best practices have emerged.

Each insurer's cyber insurance risk will vary based many factors, including the insurer's size, resources, geographic distribution, market share, and industries insured. Each insurer should take an approach that is proportionate to its risk.

Industry Guidance

◀ Strategy

Insurers should have a formal strategy for measuring cyber insurance risk that is directed and approved by senior management and the board of directors, or the governing body if there is no board.^[16] The strategy should include clear qualitative and quantitative goals for risk, and progress against those goals should be reported to senior management and the board, or the governing body if there is no board, on a regular basis. The strategy should incorporate the six key practices identified below.

2. Manage and Eliminate Exposure to Silent Cyber Insurance Risk

Insurers that offer cyber insurance should determine whether they are exposed to silent or non-affirmative cyber insurance risk, which is risk that an insurer must cover loss from a cyber incident^[17] under a policy that does not explicitly mention cyber. Even property/casualty insurers that do not explicitly offer cyber insurance should evaluate their exposure to silent risk and take appropriate steps to reduce their exposure. Silent risk can be found in a variety of combined coverage policies and stand-alone non-cyber policies, including errors and omissions, burglary and theft, general liability and product liability insurance.^[18] Cyber risk likely has not been quantified or priced into these policies, which exposes insurers to unexpected losses.

Ultimately, insurers should eliminate silent risk by making clear in any policy that could be subject to a cyber claim whether that policy provides or excludes coverage for cyber-related losses. Elimination of this risk will take some time, given the many existing policies that can contain silent cyber risk. Insurers should therefore also take steps to mitigate existing silent risk, such as by purchasing reinsurance.

3. Evaluate Systemic Risk

As part of their cyber insurance risk strategy, insurers that offer cyber insurance should regularly evaluate systemic risk and plan for potential losses. Systemic risk has grown in part because institutions increasingly rely on third party vendors and those vendors are highly concentrated in key areas like cloud services and managed services providers. Insurers should understand the critical third parties used by their insureds and model the effect of a catastrophic cyber event on such critical third parties that may cause simultaneous losses to many of their insureds. Examples of such events could include a self-propagating malware, such as NotPetya, or a supply chain attack, ^[19] such as the SolarWinds trojan, that infects many institutions at the same time, or a cyber event that disables a major cloud services provider. A catastrophic cyber event could inflict tremendous losses on insurers that may jeopardize their financial solvency.^[20]

Industry Guidance

cybersecurity stress tests based on unlikely but accurate stress testing requires accounting for both silent and affirmative risk. Moreover, because exposure to catastrophic cyber events varies across business industries and by type and size of the insured, insurers should track the impact of stress test scenarios across the different kinds of insurance policies they offer as well as across the different industries of their insureds. The cyber insurance risk strategy should account for possible losses identified in stress tests.

4. Rigorously Measure Insured Risk

Insurers that offer cyber insurance should have a data-driven, comprehensive plan for assessing the cyber risk of each insured and potential insured. This commonly starts with gathering information regarding the institution's cybersecurity program through surveys and interviews on topics including corporate governance and controls, vulnerability management, access controls, encryption, endpoint monitoring, boundary defenses, incident response planning and third-party security policies. The information should be detailed enough for the insurer to make a rigorous assessment of potential gaps and vulnerabilities in the insured's cybersecurity. Third-party sources, such as external cyber risk evaluations, are also a valuable source of information. This information should be compared with analysis of past claims data to identify the risk associated with specific gaps in cybersecurity controls.

5. Educate Insureds and Insurance Producers

Insurers that offer cyber insurance have an important role to play in educating their insureds about cybersecurity and reducing the risk of cyber incidents. Insurers should strive to offer more comprehensive information about the value of cybersecurity measures and facilitate the adoption of those measures. Insurers should also incentivize the adoption of better cybersecurity measures by pricing policies based on the effectiveness of each insured's cybersecurity program.

Several leading insurers already offer their insureds guidance, discounted access to cybersecurity services, and even cybersecurity assessments and recommendations for improvement.^[21] We commend these initiatives, and insurers should continue to expand the type, scope and reach of such offerings.

Insurers should also encourage and assist with the education of insurance producers who should have a better understanding of potential cyber exposures, types and scope of cyber coverage offered, and monetary limits in cyber insurance policies.^[22] Ensuring that the need for, benefits of, and limitations to cyber insurance are well understood and

Industry Guidance

Insurers will facilitate the growth of a robust cyber

6. Obtain Cybersecurity Expertise

Insurers that offer cyber insurance need appropriate expertise to properly understand and evaluate cyber risk. Insurers should recruit employees with cybersecurity experience and skills and commit to their training and development, supplemented as necessary with consultants or vendors.

7. Require Notice to Law Enforcement

Cyber insurance policies should include a requirement that victims notify law enforcement. Some insurers that offer cyber insurance already engage in this best practice.^[23] Notice to law enforcement may be beneficial both to the victim-insured and the public.^[24] Law enforcement often has valuable information that may not be available to private sources and can help victims of a cyber incident. Law enforcement can help recover data and funds that were lost. For instance, when funds are stolen through a business email compromise, law enforcement can sometimes block or reverse wire transfers if alerted of the incident promptly. Notice to law enforcement also can enhance a victim's reputation when its response to a cyber incident is evaluated by its shareholders, regulators, and the public. Finally, information received by law enforcement can be used to prosecute the attackers, warn others of existing cybersecurity threats, and deter future cybercrime.

[1] See NYDFS, [Guidance to Department of Financial Services \(“DFS”\) Regulated Entities Regarding Cybersecurity Awareness During COVID-19 Pandemic](#), April 13, 2020; U.S. Treasury Dep't Financial Crimes Enforcement Network (FinCEN) Advisory on Cybercrime and Cyber-Enabled Crime Exploiting the Coronavirus Disease 2019 (COVID-19) Pandemic, FIN-2020-A005, July 30, 2020.

[2] See NAIC, Report on the Cyber Insurance and Identity Theft Coverage Supplement (December 4, 2020). Note that this includes both standalone cyber insurance coverage as well as endorsements to non-cyber insurance policies.

[3] See Munich Re, [Cyber Insurance: Risks and Trends](#) (April 14, 2020).

[4] See Cyberspace Solarium Commission, [March 2020 Report](#) at 79.

[5] See 23 NYCRR 500.17.

Industry Guidance

se of the Financial System to Facilitate Ransom

) at 4 (citing FBI Internet Crime Complaint Center

reports from 2018 and 2019 for the proposition that the “severity and sophistication of ransomware attacks continue to rise” and noting that the average dollar amount in financial institution SARs on ransomware is \$783,000 thus far in 2020, an increase of \$280,000 from 2019).

[7] See Purple Sec, [2020 Ransomware Data, Statistics, and Trends](#) (2020).

[8] See OFAC, [Advisory on Potential Sanctions Risk for Facilitating Ransomware Payments](#) at 1, October 1, 2020.

[9] See Coveware, [Ransomware Demands continue to rise as Data Exfiltration becomes common, and Maze subdues](#), Nov. 4, 2020.

[10] See Cyberspace Solarium Commission, [March 2020 Report](#) at 80.

[11] See NYDFS Industry Letter -- Supply Chain Compromise Alert, December 18, 2020. See also Cybersecurity & Infrastructure Security Agency (CISA) [Alert \(AA20-352A\)](#) Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations; [CISA Emergency Directive 21-01 Mitigate SolarWinds Orion Code Compromise](#).

[12] See NYDFS Industry Letter -- Supply Chain Compromise Alert, December 18, 2020.

[13] Partner Re, [Cyber Insurance The Markets View Report](#) at 2, September 17, 2020. See also Bank of England Prudential Regulation Authority, [Letter to Chief Executives of Specialist General Insurance Firms Regulated by PRA](#), at 1, 2019 (“[f]irms almost all agreed that a number of traditional lines of business have considerable exposure to non-affirmative cyber risk”).

[14] See Jon Bateman, [War, Terrorism, and Catastrophe in Cyber Insurance: Understanding and Reforming Exclusions](#), Carnegie Endowment for International Peace, at 8-9 (October 2020).

[15] All DFS-regulated insurers also must address their own cybersecurity and comply with the cybersecurity regulations set forth in 23 NYCRR 500.

[16] See Bank of England Prudential Regulation Authority, [Cyber Insurance Underwriting Risk](#), 2017 at 6-7 (recommending that cyber risk strategy be reviewed by the Board).

[17] A “cyber incident” occurs when an unauthorized user gains access to, disrupts or misuses an organization’s information system or gains access to or misuses information stored on that system which is of value to the organization, including, but not limited to, patient records, nonpublic information, intellectual property, and customer information. An “information system”

Industry Guidance

sources organized for the collection, processing, and disposition of electronic information, as well as any

specialized system such as industrial/process controls systems, telephone switching and private branch exchange systems, and environmental control systems.

[18] See Bank of England Prudential Regulation Authority, [Letter to Chief Executives of Specialist General Insurance Firms Regulated by PRA](#), at 1-2, 2019.

[19] See Cyberspace Solarium Commission, [March 2020 Report](#) at 8 (describing the global chaos caused by the NotPetya attack in 2017 when Russian cyber operators launched a malware attack targeted at Ukrainian institutions that quickly spread to, and disabled, critical systems worldwide).

[20] See NAIC, Report on the Cybersecurity Insurance and Identity Theft Coverage Supplement, September 12, 2019 (“[a] systemic event continues to be the top threat to cyber insurers’ solvency”), citing AM Best Market Segment Report, June 17, 2019.

[21] See, e.g., American International Group (AIG), [CyberMatics](#) (providing insureds tools to manage their cybersecurity risk).

[22] See Cyberspace Solarium Commission, [March 2020 Report](#) at 80 (recommending training and certification for those in the insurance industry, emphasizing that in order for “underwriters to effectively evaluate and analyze risk in a given industry, they must understand it”).

[23] Based on DFS’s survey, 36% of insurers required their cyber insurance insureds to notify law enforcement of a cyber incident.

[24] For ransomwares incidents, OFAC will consider contacting law enforcement as a mitigating factor in case sanctions laws are violated. OFAC, [Advisory on Potential Sanctions Risk for Facilitating Ransomware Payments](#), October 1, 2020 at 4.

Who
We
Supervise

Institutions That We Supervise

The Department of Financial Services supervises many different types of institutions. Supervision by DFS may entail chartering, licensing, registration requirements, examination, and more.

[Learn More](#)

Outside Counsel

Don't Blame the Victim: A Potential Defense for Ransom Payers and Facilitators after OFAC's Ransomware Sanctions Facilitation Advisory

In October 2020, the Department of Treasury's Office of Foreign Assets Control (OFAC) issued an "Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments" (the Advisory), putting into writing guidance to reinforce the prohibition of ransom payments by ransomware attack victims to not only the defined class of Specially Designated Nationals (SDNs) targeted under Treasury's Cyber Sanctions Program—but also to a broad class of *any* entities with a "sanctions nexus" to SDNs. The Advisory, however, does not contain any insight into just what constitutes a "sanctions nexus" in the unique context of Treasury's Cyber Sanctions Program. Nevertheless, the Advisory memorializes OFAC's ability to impose strict liability on any company that makes the difficult decision to pay a ransom to protect its reputation, business secrets, personal data, and value for shareholders. What is more, the Advisory also specifically warns the ransom negotiators, insurers, and financial institutions that assist victims who make the



By
**Michael A.
Kleinman**



And
**Marc
Schein**

difficult decision to pay that they, too, may be liable for facilitating a ransom payment with the undefined "sanctions nexus."

There are plenty of good reasons not to pay a ransom, not least of which is the lack of any guaranty that a threat

At least one company recently succeeded in a judicial challenge to sanctions enforcement based on OFAC's failure to provide fair notice of what constituted sanctionable conduct under one of its (non-cyber) regulations.

actor will simply disappear, never to return. But in many instances, without paying, management will be unable to run its business or deliver its goods and services. The decision not to pay can be devastating. For example, when a SamSam attack hit the City of Atlanta

in March 2018 (an incident referenced in the Advisory), the City elected not to pay the \$51,000 demanded for decryption. The result was an inability to work around the encryption and a cost of \$17 million to rebuild its network.

Ignoring such real world consequences, the Advisory's reminder that OFAC imposes strict liability for payments to those with an undefined "sanctions nexus" coupled with the unique inability to identify all prohibited individuals and the digital currency accounts they use to receive a ransom leaves ransomware victims, who desperately need the comfort of certainty after an attack, with no comfort at all.

While many commentators have reacted to the Advisory by stressing the importance of implementing robust screening and compliance measures and warning companies to do their best to avoid paying ransoms, we focus on how to mount a defense to a potential sanctions enforcement action under the Advisory when some or all of those efforts have been taken to no avail.

Background Leading Up to OFAC's October 2020 Ransomware Advisory. In response to the proliferation of ransomware attacks over the last five years in particular, a series of Executive Orders and statutes, as further codified by OFAC in its regulations and

MICHAEL A. KLEINMAN is a special counsel of Fried, Frank, Harris, Shriver & Jacobson. MARC SCHEIN, CIC, CLCS, is the National Co-Chair, Cyber Center of Excellence at Marsh & McLennan Agency. BRYAN A. MCINTYRE, an associate at Fried Frank, assisted in the preparation of this column.

explained in advisories, have come to include cyberterrorists amongst the list of banned individuals with whom U.S. persons cannot conduct financial transactions. See, e.g., U.S. Dep't of Treas., *Sanctions Related to Significant Malicious Cyber-Enabled Activities*.

In 2015, President Obama issued Executive Order 13694 (E.O. 13694) titled "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities," which, among other things, authorized the imposition of sanctions against any person responsible for or complicit in, directly or indirectly, engaging in "malicious cyber-enabled" activities that are "reasonably likely to result in, or have materially contributed to, a significant threat to the national security ... of the United States." The list of cyber activity subject to sanctions is incredibly broad in scope and includes: "causing a significant disruption to the availability of a computer or network(s) of computers; [] causing a significant misappropriation of funds or economic resources, trade secrets, personal identifiers, or financial information;" or any other activity that disrupts computer infrastructures or threatens access to an entity's vital information. 80 Fed. Reg. 18077 (April 1, 2015).

In accordance with E.O. 13694, Treasury implemented its "Cyber-Related Sanctions Regulations" (31 C.F.R. §§578 et seq.) on Dec. 31, 2015 (the Regulations), giving birth to OFAC's Cyber Sanctions Program. As is common for "list-based" sanctions programs, the Regulations offered little interpretative guidance to E.O. 13694's broad language, merely incorporating the E.O. by reference. Nor has any subsequent guidance issued by Treasury provided any more clarity until the Advisory.

For example, the 15 Cyber-Related FAQs maintained on Treasury's website as of Feb. 2, 2021 focus on: developing a tailored, risk-based compliance program that *may* include screening "or other appropriate measures;" clarifying certain exclusions from the Regulations, such as American whistleblower activity, provision of legal advice, and network defense; and noting that a general license allows certain transactions with the Russian Federal Security Service. Notably, despite the acceleration of ransomware attacks in the last few years, there has been no new Cyber-Related FAQ posted since November 2018. See U.S. Dep't of Treas., *Frequently Asked Questions, Cyber-Related Sanctions*.

There are plenty of good reasons not to pay a ransom, not least of which is the lack of any guaranty that a threat actor will simply disappear, never to return. But in many instances, without paying, management will be unable to run its business or deliver its goods and services. The decision not to pay can be devastating.

Aside from the Advisory and the FAQs, the only other guidance published by Treasury on its Cyber-Related Sanctions Program is a document entitled "Sanctions Against Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities," which was last updated in July 2017 (the Guidance). In large part, the Guidance merely summarizes existing authorities and potential penalties. There are, however, two notable highlights. First, the Guidance itself characterizes the Regulations as "abbreviated" but states that "OFAC

intends to supplement the Regulations with a more comprehensive set of regulations, which may include additional interpretative and definitional guidance and additional general licenses and statements of licensing policy." Yet no supplemental regulations have been implemented. Second, the Guidance states that special licenses to authorize otherwise banned transactions will be considered on a case-by-case basis, but does not provide any criteria for how to make a decision.

In light of the limited guidance and dearth of specific regulations covering OFAC's Cyber Sanctions Program, word of the October 2020 Advisory should have been welcome news to the cyber and international trade communities. Unfortunately, however, the Advisory created more questions than it answered.

How Companies Should Think About the Advisory. Coming on the heels of an increase in demand for ransomware payments during the COVID-19 pandemic, the Advisory signals OFAC's intent to more actively regulate the flow of funds to threat actors out of a fear that those who perpetrate the attacks may be using the proceeds to fund "activities adverse to the national security and foreign policy objectives of the United States." But it is not just victims that need be concerned. The Advisory also specifically calls out financial institutions, cyber insurance firms, and companies involved in digital forensics and incident response for encouraging future ransomware payment demands by helping victims pay to recover access to their data.

The Advisory reiterates that OFAC has the authority to issue civil penalties to and refer for criminal investigation and/or prosecution under the International Emergency Economic

Powers Act and the Trading With the Enemy Act *any* companies negotiating ransomware payments with those “designated [as] malicious cyber actors under [OFAC’s] cyber-related sanctions program,” as well as those who have a “*sanctions nexus*” to these actors. But the number of cyber actors on the SDN list, particularly when considering the undefined “sanctions nexus,” is truly unknowable. As of Jan. 19, 2021, the SDN list includes at least 130 known cyber threat actors, generally with one or more digital currency wallet addresses. But this list is just the tip of the iceberg of those who move below the surface on the Dark Web. Anonymous threat actors are notorious for working in groups or syndicates with other individuals or affiliates. And worse yet, in the last few years, “Ransomware as a Service” offered by several notorious syndicates has served to create a diaspora of unknown threat actors who buy or lease ransomware variants to deploy their own attacks.

Put simply, while there is a long list of threat actors and wallet addresses that companies can screen to determine if they can proceed with payment, the Advisory’s addition of those individuals who post hoc are found by OFAC to have had a “sanctions nexus” to an SDN adds to the list of prohibited individuals a group of threat actors that would have slipped through reasonable screening programs maintained by victims and their advisors. Indeed, if OFAC later determines that the threat actor was an SDN, otherwise blocked, or located in a sanctioned country, the victim and its advisors will have violated the Regulations regardless of *any* screening the victim performed.

Victims who have run the screens and followed responsible incident response plans, yet still pay actors

later deemed to have a sanctions nexus to a blocked entity by OFAC, thus will be put in an impossible situation: Don’t pay and risk potentially material operational, reputational, and monetary consequences, or roll the dice and pay the perpetrator, then potentially pay OFAC again after innocently entering the unknown realm of the “sanctions nexus” (and *still* risk potentially material operational, reputational, and monetary consequences).

While the Advisory makes clear that credit will be given to those ransom payers who undertake mitigation efforts such as maintaining robust compliance programs and making self-initiated, timely, and complete reporting of an attack to law enforcement, the Advisory does not provide any clarity on how such mitigation efforts will avoid fines for payments involving the “sanctions nexus” other than to say that notification and cooperation with law enforcement will be seen as “significant.”

On the other hand, what is clear from the Advisory is that a “specific” OFAC license, which would bless an otherwise unlawful payment, is all but foreclosed. First, the Advisory states that any license application will be met with a “presumption of denial.” Second, in any event, since the typical victim has a matter of days to decide to pay a ransom and the OFAC license application process can take weeks or months, an OFAC license is for all intents out of the question.

One collateral effect of the Advisory’s specific warning to cyber insurers who assist victims who decide to pay ransoms may be an increase in coverage denials for ransom payments made by or on behalf of insureds. It is critical that management understands how the company’s cyber insurance

policies may respond to a ransomware event. In particular, management must understand the difference between the “pay on behalf of” and “reimbursement” clauses in their cyber insurance policies. As ransomware attacks have escalated in the recent past, ransom demands exceeding \$1 million have become commonplace, with some demands exceeding \$10 million. This is also evidence showing that average ransom payments across all industries increased in the third quarter of 2020, and that cyber insurance claims are rising drastically. Increased regulatory scrutiny signaled by the Advisory combined with the increase in ransomware attacks may lead to an elimination of the “pay on behalf of” option, resulting in a large out of pocket expense that not all businesses can afford. Moreover, the new “sanctions nexus” language in the Advisory may vitiate coverage for OFAC penalties and related losses under a reimbursement clause altogether, when coupled with a sanctions limitation or exclusion clause. Indeed, the cyber insurance market has already tightened in response to the uptick in ransomware claims. Carriers are now requiring supplemental coverage applications to procure ransomware and cyber extortion insurance, and putting in place sublimits for such coverage parts. What is more, several carriers have left the market altogether. Finally, on Feb. 4, 2021, the New York State Department of Financial Services issued an Insurance Circular Letter addressed to all property and casualty insurers, citing the Advisory and an increase in ransomware incidents, and warning insurers that they too can be liable for ransom payments made to sanctioned entities. The letter set forth a new Cyber Insurance Risk Framework outlining best practices

that insurers who write cyber insurance policies should take to manage more effectively their own risks to potentially “massive” claim losses.

Can Companies Defend Themselves Against the ‘Sanctions Nexus’? Whether or not a ransom payment is ultimately covered by insurance, what defense is available to a victim or facilitator who has run the screens, attempted the mitigating factors suggested by OFAC, and made the difficult decision to pay a non-SDN threat actor that nevertheless later turns up to have a “sanctions nexus”?

At least one company recently succeeded in a judicial challenge to sanctions enforcement based on OFAC’s failure to provide fair notice of what constituted sanctionable conduct under one of its (non-cyber) regulations. In *Exxon Mobil v. Mnuchin*, Exxon filed an action against the Secretary of the Treasury and OFAC challenging a \$2,000,000 fine imposed on Exxon for doing business with a non-SDN company, whose president and chairman had been designated as an SDN “in his individual capacity.” 430 F. Supp. 3d 220, 226 (N.D. Tex. 2019). There, Exxon’s entry into a series of contracts with the company, signed by the SDN, as president, without seeking pre-approval from OFAC was deemed to be prohibited conduct.

The regulation at issue in *Exxon* provided that a U.S. company could not receive “services” from individuals or entities identified on OFAC’s SDN list. Exxon asserted that OFAC’s failure to define “receipt of services” was a violation of the Due Process Clause of the Fifth Amendment. *Id.* at 229. In response, OFAC contended that Exxon clearly received services from a SDN because the SDN signed the contracts on behalf of the company, and the

signature of the SDN clearly constituted the receipt of services from the SDN. *Id.* at 231-32.

Noting that “fair notice” in the administrative agency context required OFAC to provide “‘ascertainable certainty’ of its interpretation of the Regulations,” the court found that neither the Regulations nor any other OFAC guidance served to put Exxon on notice that the SDN’s execution of the contract in his corporate capacity would constitute a “receipt of services.” *Id.* at 233. Clearly recognizing the inherent vagaries in that sanctions program, the court colorfully framed the issue as a determination of “which party receive[d] the benefit of having its cake and eating it, too—the regulating agency that failed to clarify, or the regulated party that failed to ask.” *Id.* at 225.

In the cyber context, the vague description of “sanctions nexus,” which is absent from the Executive Orders, the FAQs, and the Guidance, does not clear the ultimate hurdle of “ascertainable certainty” required by the Fifth Amendment. That is, just as OFAC sought to justify an enforcement action based on the “receipt of services” language in *Exxon*, any finding of liability for payments to a non-SDN based on the cyber Regulations would force OFAC to justify cyber-related sanctions based on undefined “sanctions nexus” language. To date, the term “sanctions nexus” is *only* contained in the Advisory, and OFAC purports to define fully the term in a matter of a few sentences in the Advisory containing non-exhaustive hypotheticals. In *Exxon*, the court rejected OFAC’s argument that the “sweeping language” it used had a “common meaning” that justified sanctions despite the absence of any public statements clarifying its meaning. *Id.* at 232. The Advisory

and the scant additional public statements by OFAC on its Cyber Sanctions Program should fair no better when subject to judicial scrutiny. That is, a court applying *Exxon* to the “sanctions nexus” language should likewise hold that the Regulations are vague, overly “broad,” and that the OFAC guidance “fails to delineate their boundaries.” *Id.* at 243.

Accordingly, *Exxon* can well serve as a roadmap for a defense to sanctions enforcement against a ransomware victim and its advisors premised on nothing other than a “sanctions nexus.” While the *Exxon* decision is far from precedential given it represents just one district judge’s opinion in the very rare occasion where a party challenged OFAC sanctions in district court—let alone successfully, it provides a path to a potential defense for victims and their advisors who make the difficult choice to work together to pay an unknown threat actor.