Cybersecurity and Data Privacy for Law Firms

September 21, 2023

Patrick Fitzsimmons ’09, Partner, Hodgson Russ LLP
Michelle Merola, Partner, Hodgson Russ LLP
Amanda Pike, FBI Special Agent, Buffalo Cyber Task Force

Law Firms Are in The Headlines

Law Firm Data Breaches Surge In 2023

ABOVE THE LAW

Bloomberg Law

Law Firm Cyberattacks Grow, Putting Operations in Legal Peril

THE AMERICAN LAWYER

Cyberattacks 'Inevitable' for Law Firms, Highlighting Need for Comprehensive Incident Response Plans

Hodgson Russ LLP ATTORNEYS

Today's Agenda

- Introductions
- Current Legal Landscape
- Law Firm Compliance
- Law Enforcement Perspective

Hodgson Russ LLP ATTORNEYS

Legal Patchwork of Laws (and regulators)

Ethical Rules	International Law	US Federal Laws are Industry Specific	US State Privacy Laws	State Breach Notification Laws
• ABA Model Rules • New York Rules of Professional Conduct	• GDPR • UK GDPR • PIPEDA • Brazil	• HIPAA • GLBA • CAN-SPAM • FTCA • COPPA	• California • Colorado • Connecticut • Virginia	• NY SHIELD Act • All other states

- These are simply a few examples. Currently, the legal landscape in the United States is a patchwork of federal sector-specific laws and 50 different state laws. There is no comprehensive federal privacy law in the U.S., but there is legislation pending that could change that (*e.g.*, American Data Privacy and Protection Act).

Hodgson Russ LLP ATTORNEYS

What Inspired the Emergence of US Privacy Law?
General Data Protection Regulation (E.U.)

- Requires transparency so that data subjects are informed what data is being collected and what it is used for.
- Provides data subjects with access to their personal data upon request and the right to have data corrected or deleted.
- Businesses must have a lawful purpose to collect data.
- Businesses need to ensure that only the data necessary for the lawful purpose is collected and that the collected data is retained no longer than necessary for that lawful purpose (i.e., minimization requirement).

U.S. Federal Laws

- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
  - Regulates protected health information
  - Includes both privacy rights and standards to safeguard protected health information
  - Notice Obligations (ransomware is presumptive breach)
- Children's Online Privacy Protection Act of 1998 (COPPA)
  - Designed to protect the privacy of children under the age of 13
  - Certain websites must include privacy policies that describe the information collected from users
- Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act)
  - Regulates commercial emails. A commercial email is "any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service."
  - Must permit consumers to opt-out through the use of an unsubscribe button.

- No GDPR-like federal legislation in the United States, but there is some pending legislation that could change that.

New York SHIELD Act (breach notification)

- Covers two key areas: (1) breach notification and (2) data security
- “Personal Information” means any information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such natural person.
- “Private Information” means personal information plus another data element listed in the statute such as a social security number, driver’s license number, or biometric information, among other things. It also includes an email address in combination with a password or security question and answer that would permit access to an online account.
- Breach is defined as unauthorized “access to or acquisition of” private information (subject to some exceptions).
- Any business owning or licensing computerized data that includes private information must notify any resident of New York whose private information was accessed or acquired and must also notify the Attorney General, the Department of State, and the State Police.

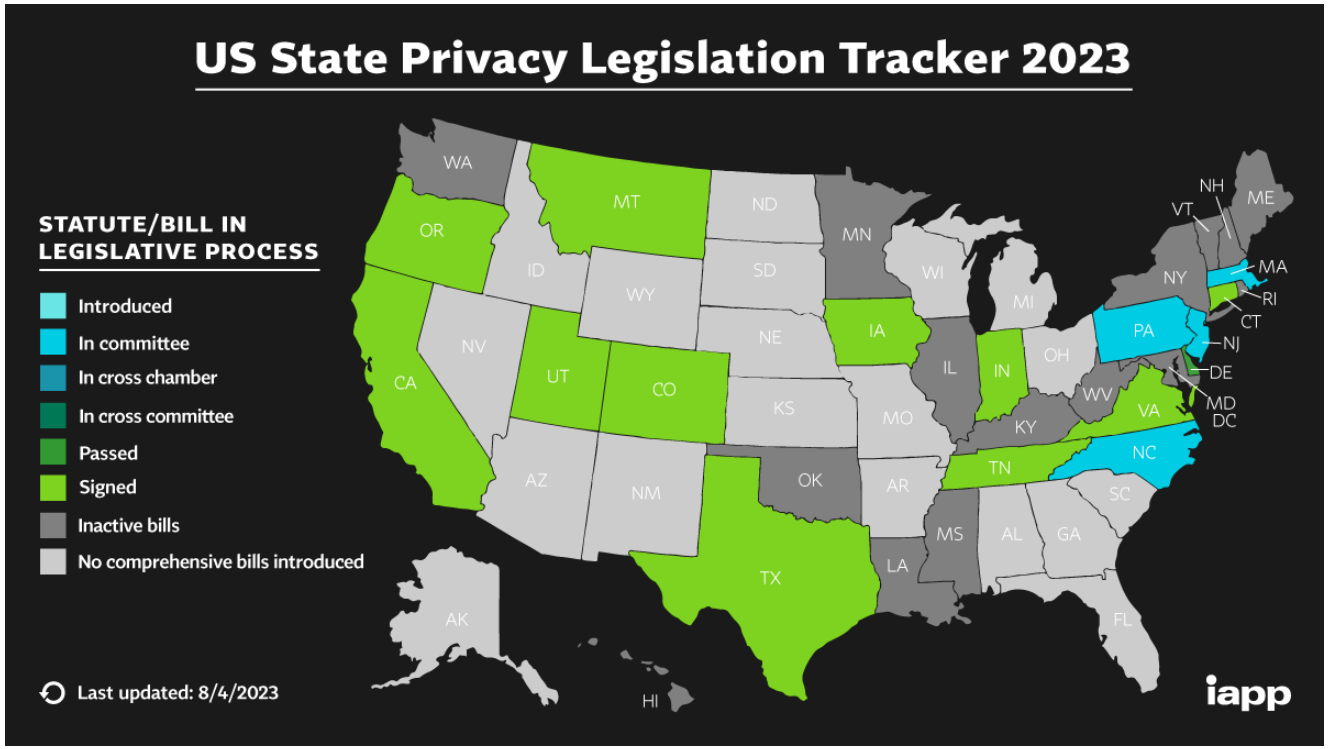
New York SHIELD Act cont'd (data security)

- The SHIELD Act also imposes data security obligations on businesses.
- Businesses must implement and maintain reasonable safeguards to protect the security, confidentiality, and integrity of private information. To do so, the business must implement reasonable administrative, technical, and physical safeguards. The SHIELD Act lists various safeguards for businesses to implement.
- For small businesses (defined as less than 50 employees, less than three million dollars in gross annual revenue in each of the last three fiscal years, or less than five million in year-end total assets) the statute's menu of safeguards does not necessarily apply.
- Instead, the SHIELD Act says that a small business must have reasonable administrative, technical, and physical safeguards that "are appropriate for the size and complexity of the small business, the nature and scope of the small business's activities, and the sensitivity of the personal information the small business collects from or about consumers."

Emergence of State Laws

As of today, twelve U.S. states have enacted comprehensive data privacy laws:

- California (1/23)
- Colorado (7/23)
- Connecticut (7/23)
- Delaware (1/25)
- Indiana (1/26)
- Iowa (1/25)
- Montana (10/24)
- Oregon (7/24)
- Tennessee (7/25)
- Texas (7/24)
- Utah (12/31/23)
- Virginia (1/23)



But many more to come . . .
including New York

(All states have breach notification laws.)

Hodgson Russ LLP ATTORNEYS

California Consumer Privacy Act (CCPA)

- Consumer Rights Statute
- Applies to for-profit businesses that do business in California and meet any of the following criteria (thresholds as of Jan. 1, 2023):
  - Gross annual revenues over $25 million
  - Buy, sell, or share the personal information of 100,000 or more consumers or households
  - Derive 50% or more of their annual revenue from selling or sharing consumers' personal information
- Doing business is broadly defined.
- Privacy policies must contain California-specific provisions.

California Privacy Rights Act (CPRA)

- Amends the CCPA and went into effect January 1, 2023
- Enhances the rights of consumers and the corresponding obligations of businesses
- Establishes a new sub-category of personal information called “sensitive personal information”
  - *e.g.,* SSN, state identification card, precise geolocation information, racial or ethnic origin, and biometric identification, among other things
  - Businesses collecting sensitive personal information are required to notify consumers at or before the time of collection of (1) the category of information collected; (2) the retention period; and (3) whether such information is sold by the business.
- CPRA extends its reach to employees’ personal information and personal information shared among businesses
- Draft regulations require businesses to conduct annual risk assessments that identify and address gaps in various security controls, including multifactor authentication, passwords, encryption, zero-trust architecture, privilege restrictions, secure configuration, patch management, logging and more.

Data Privacy vs. Privilege and Confidentiality

New York Rule of Professional Conduct 1.6 addresses confidentiality of information relating to the representation of a client. Evidentiary privileges govern communications between attorney and client and attorney work product. There are also times when attorneys must maintain confidentiality of non-client information under a protective order or other confidentiality agreement.

We are lawyers, so we have this privacy thing covered?

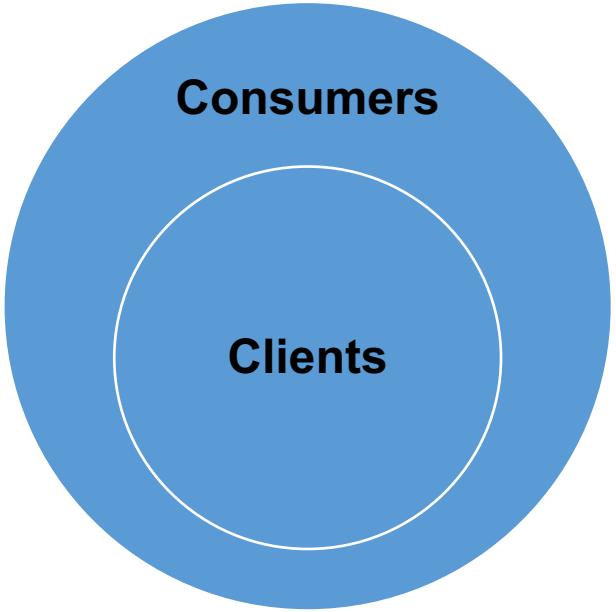
. . . maybe not!

New York Rules of Professional Conduct

- Rule 1.1 – Competence
  - Comment 8 requires the lawyer to stay abreast of the benefits and risks associated with technology the lawyer uses to provide services to clients or to store or transmit confidential information.
- Rule 1.4 (b) – Communication
  - A lawyer shall explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation.
  - ABA Formal Opinion 483: When a data breach occurs involving, or having a substantial likelihood of involving, material client information, lawyers have a duty to notify clients of the breach and to take other reasonable steps consistent with their obligations under these Model Rules.
- Rule 1.6 (c) – Confidentiality
  - A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure or use of, or unauthorized access to, information protected by Rules 1.6, 1.9(c), or 1.18(b).
  - Comment 16 requires a lawyer to make reasonable efforts to safeguard confidential information against inadvertent or unauthorized disclosure to a third party.
  - ABA formal opinions suggest a series of steps deemed reasonable, i.e., annual risk assessment, network security audits, written information security programs, secure disposal and data retention . . .

The Protections Cover Different Groups

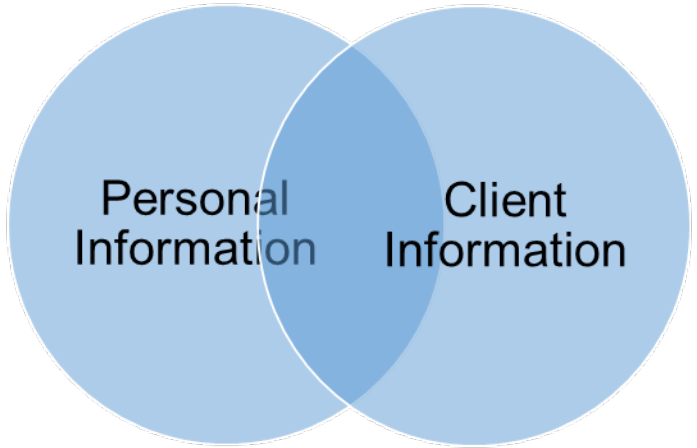
- Privilege and confidentiality obligations apply to the collection of **client** information.
- Data privacy laws apply to the collection of "personal information" of **"consumers,"** which may include not only clients but also opposing parties and third parties.



Hodgson Russ LLP ATTORNEYS

The Protections Cover Different Data

- Privilege is an evidentiary rule protecting a lawyer's communications with their client from disclosure during litigation or another proceeding.
- Client information confidentiality is broader and may include any information a lawyer has relating to a client's representation.
- Personal information, on the other hand, is information "that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular" consumer or household.

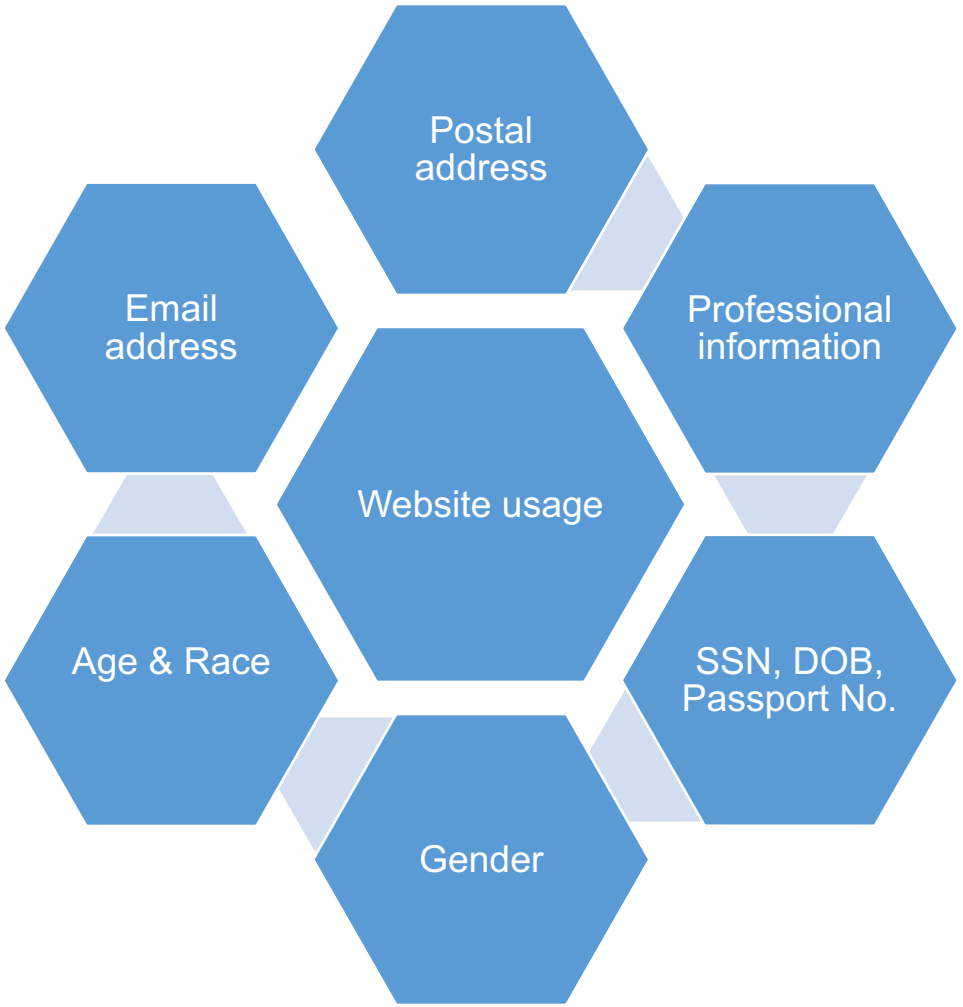


Categories of Personal Information

Categories	Example
Identifiers	Real name, alias, postal address, unique personal identifier, online identifier, IP address. Email address, account name, social security number, driver's license number or passport number
Personal Information categories listed in the California Customer Records statute	Name, signature, social security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, employment, employment history, bank account number, credit card number, debit card number, or any other financial information
Characteristics of protected classifications under California or Federal law	Gender or date of birth
Commercial Information	Records of products purchased or considered or other purchasing or consuming histories or tendencies
Biometric Information	Fingerprints or voiceprints
Internet/Electronic Activity	Browsing history, search history and interaction with a website or application
Geolocation Data	Device location
Audio, electronic, visual, thermal or olfactory information	Images and audio, video or call recordings created in connection with business activities
Professional or Employment Data	Business contact details in order to provide you our services at a business level, job title as well as work history and professional qualifications if you apply for a job with us
Education Information	Student records
Inferences drawn from other personal information	Information reflecting an individual's preferences and characteristics
Sensitive Personal Information	A consumer's social security , driver's license, state identification card, or passport number; account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account; a consumer's precise geolocation; a consumer's racial or ethnic origin, religious or philosophical beliefs, or union membership; contents of a consumer's mail, email, and text messages unless the business is the intended recipient of the communication; or a consumer's genetic data.

Hodgson Russ LLP ATTORNEYS

Personal Information in a Law Office



Obligations Under Privacy Laws

- **Notice/disclosure**
  - ✓ Privacy Policies and Engagement letters
  - ✓ consent

- Consumer requests

- **Security**
  - ✓ Risk assessments

- Opt out/in of sales

- **Recordkeeping**
  - ✓ Retention
  - ✓ Vendor contracts

- Equal treatment

- Training

Hodgson Russ LLP ATTORNEYS

NOTICE: Covered Business Must Have a Privacy Policy

Covered businesses, including law firms, are required to notify consumers about their privacy practices through the publication of readily accessible privacy policies that disclose:

1. **How information will be collected and how it will be used/shared.**
2. **A list of the following consumer privacy rights:**

- The ***right to know*** about the personal information a business collects about them and how it is used and shared;
- The ***right to delete*** personal information collected from them (with some exceptions);
- The ***right to opt-out*** of the sale of their personal information;
- The ***right to non-discrimination*** for exercising their CCPA rights; and
- The ***right to correct*** personal information.

Hodgson Russ LLP ATTORNEYS

NOTICE: Covered Business Should Address Privacy in Engagement Letters

- During the course of this engagement, the Firm may collect certain personal information relating to the services contemplated by this letter. The collection of any such personal information will be governed by, and such personal information will be processed in accordance with, the Firm's Privacy Policy, as well as any applicable privacy laws and codes of professional conduct. You can obtain a copy of the Firm's Privacy Policy on our website or by requesting one from me.
- Countersigned?

Privacy Policy and Engagement Letters are Means of Obtaining Consent to Process Personal Information

What is consent?

Any freely given, specific, informed and unambiguous indication of an individual's agreement to the processing of personal data relating to him or her.

Types:

- Opt-in and Opt-out: Opt-in systems require consent prior to processing personal data.
- Affirmative/Explicit Consent: An individual "signifies" his or her agreement by some active communication between the parties.
- Implicit Consent: Implied consent arises where consent may reasonably be inferred from the action or inaction of the individual, ex., consent inferred from use of website.

Consent Under Privacy Laws

- Unlike the GDPR (opt-in consent), the CCPA doesn't generally require advance/prior consent. (opt-out consent)
- If you provide notice of your data handling practices at the time of collecting the data, and provide the opportunity to opt-out of the collection, you can collect and use the data right away without any confirmation from the person.
- BUT READ THE FINE PRINT

  - Exceptions and Limitations on opt-out consent: Prior consent must be obtained to sell the personal information for individuals under 16.
  - "**Limit the Use of My Sensitive Personal Information**" (SPI) businesses must give notice to consumers how they use sensitive personal information and must include "a clear and conspicuous" link that will let the consumer limit certain uses and disclosures of SPI.

SECURITY: Data Protection Requirements and Security Breaches

- Many privacy laws require that businesses "implement reasonable security procedures and practices appropriate to the nature of the personal information to protect the personal information from unauthorized or illegal access, destruction, use, modification, or disclosure."

- If a business violates its duty to maintain reasonable security procedures and practices, the business may be liable for civil damages.

- Some privacy laws (like CCPA) provide a private right of action to apply to data breaches that include email addresses in combination with a password or security question/answer that permit access to the account.

Annual Cybersecurity Audits and Risk Assessments

- A risk assessment evaluates risks that a business faces with respect to the data it processes by analyzing threats and vulnerabilities. In an information security context, risk assessments are crucial for mitigating risk by proactively addressing the ways threat actors and employees might compromise sensitive information.

Hodgson Russ LLP ATTORNEYS

Risk Assessments Required by the CPRA

- The CPRA mandates that regulations developed require businesses to ***submit*** to the CPPA on a "regular basis" their risk assessments.
- The risk assessment must analyze and consider:
  - Does the processing involve sensitive personal information?
  - Do the benefits resulting from the processing outweigh the potential risks to the rights of the consumer associated with such processing?
  - Does the business need to avoid certain processing activities if they place significant potential risks on data privacy, outweighing its overall benefits?
- The precise nature of these obligations are being developed in draft regulations.

Record Keeping: Data Retention and Vendor Contracts

- Privacy laws (like CCPA) require that you keep data for no longer than necessary. Specifically, retention "shall be reasonably necessary and proportionate to achieve the purposes" for which it was collected or processed.
- Moreover, the data collected for one purpose must not be processed for other purposes.
- Privacy Laws (like CCPA) impose contracting requirements for transfers of personal information to other entities.

Hodgson Russ LLP ATTORNEYS

What Must the Contracts Include?

- Specify that the personal information is sold or disclosed only for limited and specified purposes.
- Obligates the contractor to comply with applicable obligations of the privacy law and provide the same level of privacy protections.
- Requires the contractor to notify the business if it determines it can no longer meet its obligations.
- Requires the contractor to enter into a contract with any sub-processor that contains the same privacy and security obligations.
- Grants the business rights to take reasonable and appropriate steps to ensure that the contractor uses the personal information in a manner consistent with the business's requirements/obligations.
- Grants the business the right, upon notice, to take reasonable and appropriate steps to stop and remediate unauthorized use of personal information.
- Requires the contractor certifies that it understands the restrictions on it and will comply with them.

Vendor Contracts – Other Considerations

- Review implementing regulations which provide detail regarding vendor contracts and should be reviewed to ensure full compliance.
- Indemnification and Limitation on Liability
- Insurance
- Contract should be broad enough to ensure all other jurisdictions' requirements are met (i.e., other states; GDPR; etc.)

Consequences of Failing to Obtain a Valid Contract

- In the absence of a proper contract, transfers of personal information to contractors may be deemed improper "sales/information sharing" that trigger a consumer's right to opt out and the business must provide consumers the opportunity to do so.

Federal Bureau of Investigation
Buffalo Division

The Year in Review: Cyber Trends

September 21, 2023

Total Losses

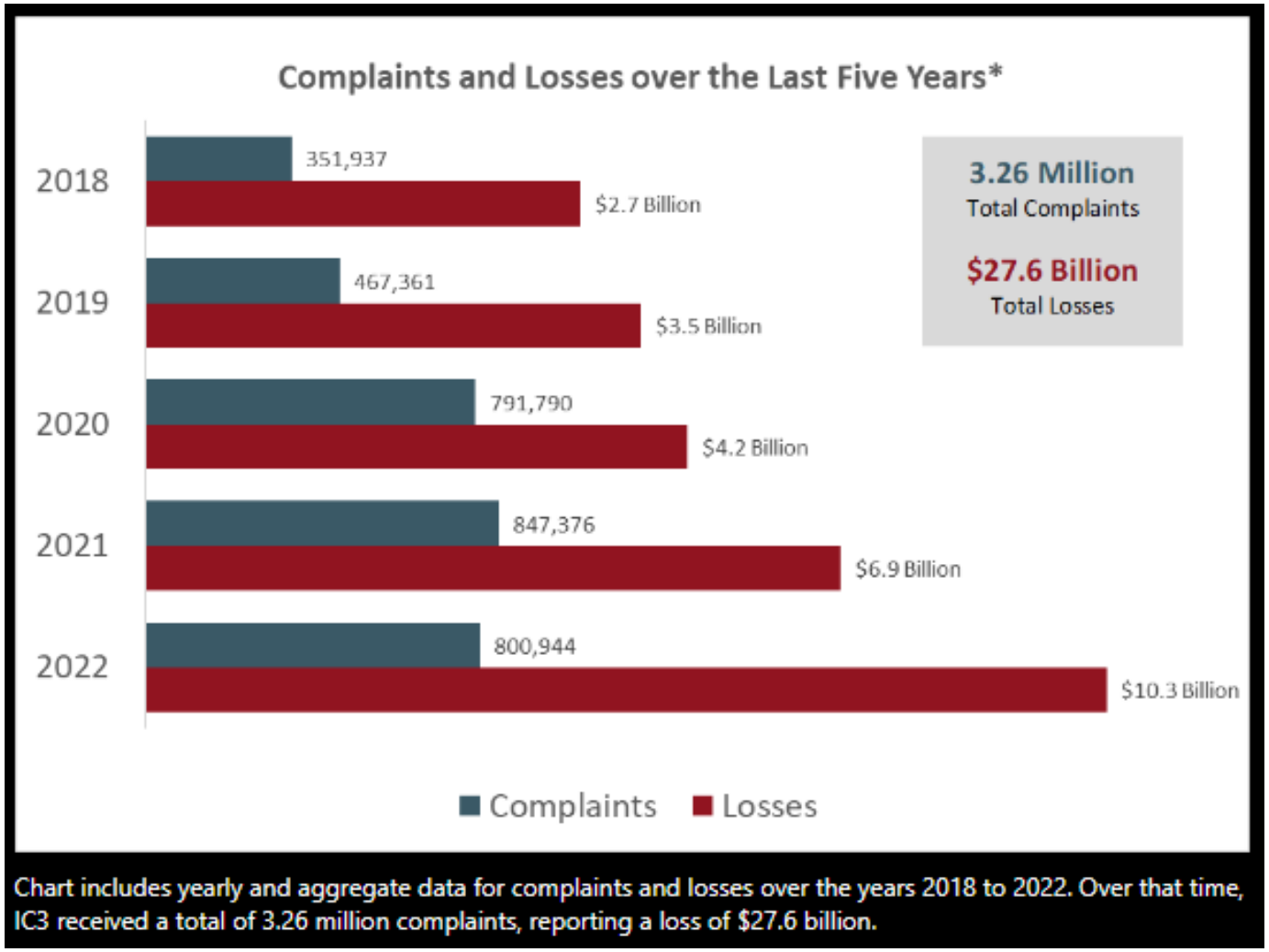


Chart includes yearly and aggregate data for complaints and losses over the years 2018 to 2022. Over that time, IC3 received a total of 3.26 million complaints, reporting a loss of $27.6 billion.

Source:
ic3.gov

Hodgson Russ LLP ATTORNEYS

Top 5 Reported Crimes

- Tech Support
  - 2022 Complaints: 32,538
- Extortion
  - 2022 Complaints: 39,416
- Non-Payment/Non-Delivery
  - 2022 Complaints: 51,679
- Personal Data Breach
  - 2022 Complaints: 58,859
- Phishing
  - 2022 Complaints: 300,497

Source:
ic3.gov

Top Threats for 2022: Business Email Compromise (BEC)

- **Threat:** 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.

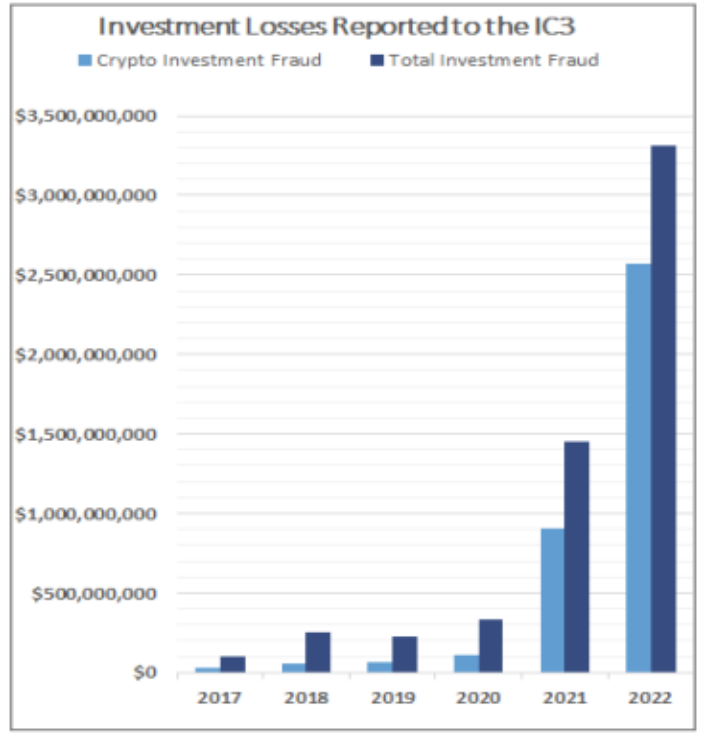
- **Trends:**
  - Fraudsters are more frequently utilizing custodial accounts held at financial institutions for cryptocurrency exchanges
  - In 2022, the IC3 also saw a slight increase of targeting victims' investment accounts instead of the traditional banking accounts.
  - There was also an increasingly prevalent tactic by BEC bad actors of spoofing legitimate business phone numbers to confirm fraudulent banking details with victims.

Source:
ic3.gov

Top Threats for 2022: Investment

- **Threat:** In 2022, investment scams were the costliest scheme reported to the IC3. Variations of crypto-investment scams reported in 2022 included Liquidity Mining, Hacked Social Media, Celebrity Impersonation, Real Estate Professionals, and Employment.

- **Trends:**
  - Unprecedented increases in the number of victims and the dollar losses to these investors.
  - Many victims have assumed massive debt to cover losses from these fraudulent investments.
  - Most targeted age group reporting this type of scam are victims ages 30 to 49.



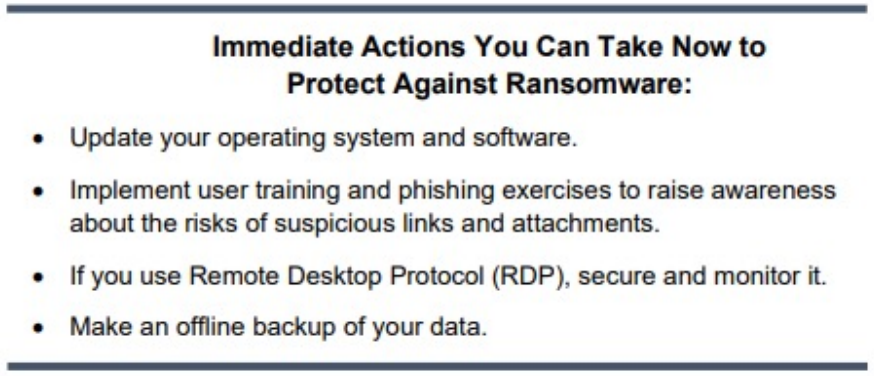
Source: ic3.gov

Hodgson Russ LLP ATTORNEYS

Top Threats for 2022: Ransomware

- **Threat:** Ransomware is a type of malicious software, or malware, that encrypts data on a computer, making it unusable. In addition to encrypting the network, the cyber-criminal will often steal data off the system and hold that data hostage until the ransom is paid. If the ransom is not paid, the victim's data remains unavailable.

- **Trends:**
  - Top Initial Infection Vectors.
  - Increase in extortion tactic.



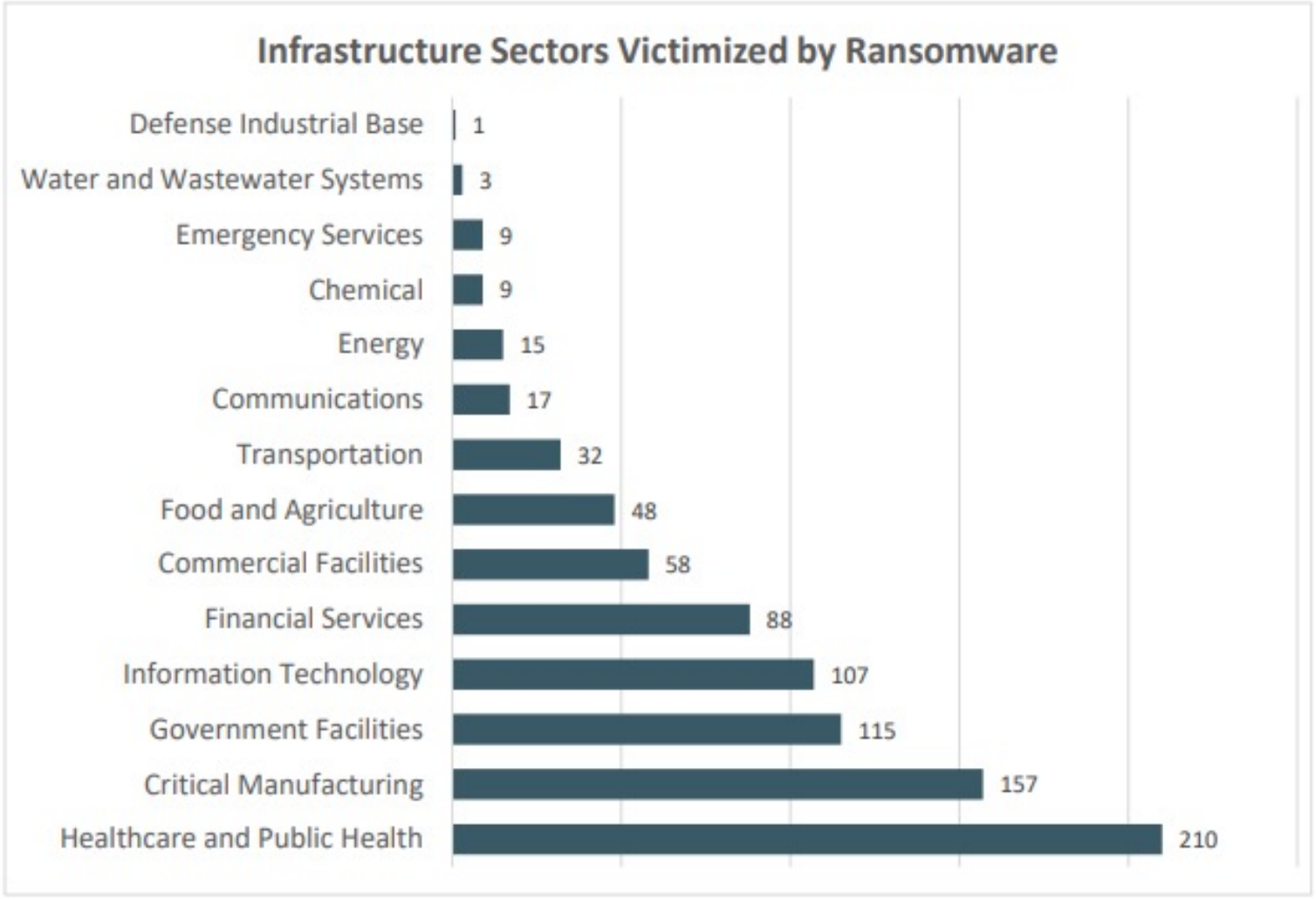
Immediate Actions You Can Take Now to Protect Against Ransomware:

- Update your operating system and software.
- Implement user training and phishing exercises to raise awareness about the risks of suspicious links and attachments.
- If you use Remote Desktop Protocol (RDP), secure and monitor it.
- Make an offline backup of your data.

Source: ic3.gov

Hodgson Russ LLP ATTORNEYS

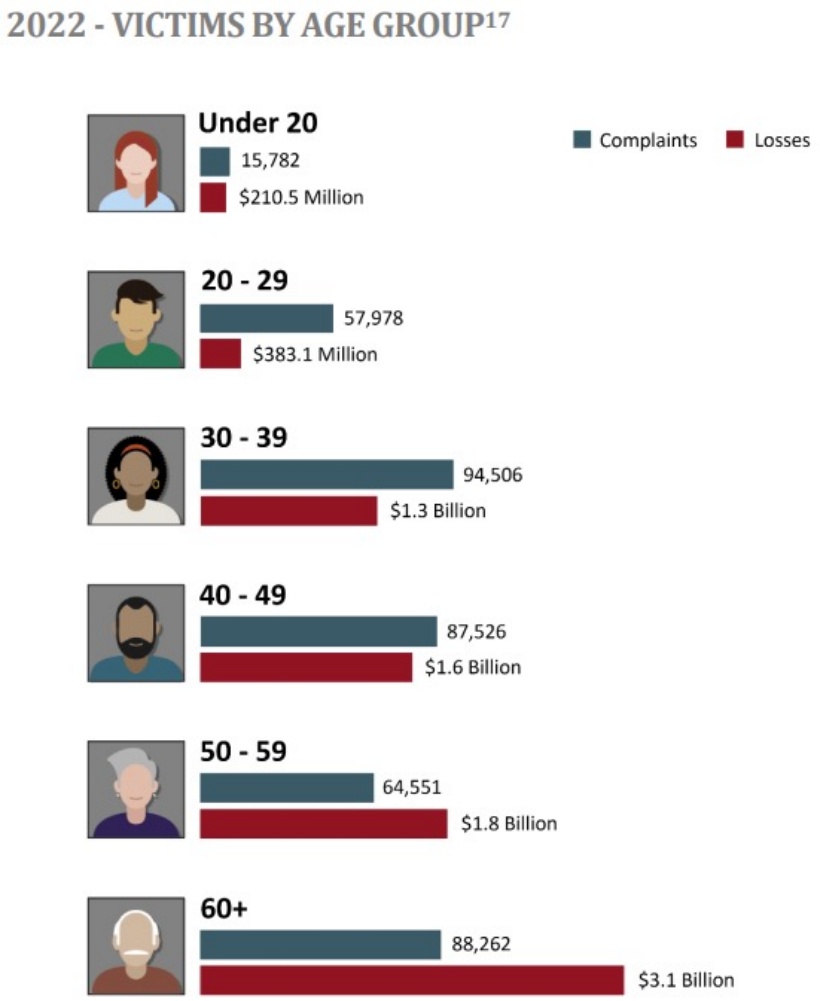
Ransomware Targets



Source:
ic3.gov

Hodgson Russ LLP ATTORNEYS

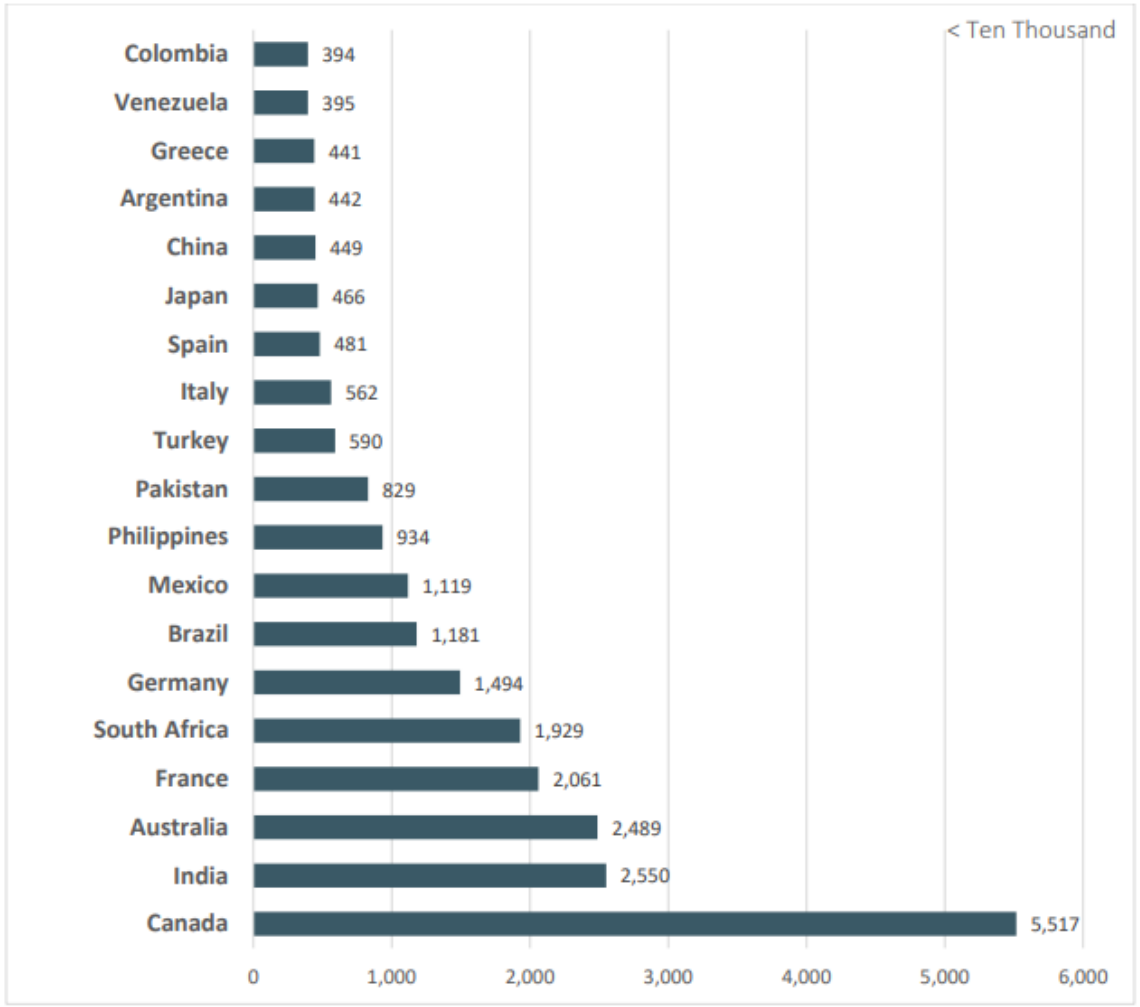
Victim Demographics



Source:
ic3.gov

Hodgson Russ LLP ATTORNEYS

2022 Top 20 International Victim Countries



As compared to:

- **U.K - 284,297**
- **U.S. - 479,101**

Source:
ic3.gov

Hodgson Russ LLP ATTORNEYS

2022 Crime Types by Victim Count

2022 CRIME TYPES

By Victim Count			
Crime Type	*Victims*	*Crime Type*	*Victims*
Phishing	300,497	Government Impersonation	11,554
Personal Data Breach	58,859	Advanced Fee	11,264
Non-Payment/Non-Delivery	51,679	Other	9,966
Extortion	39,416	Overpayment	6,183
Tech Support	32,538	Lottery/Sweepstakes/Inheritance	5,650
Investment	30,529	Data Breach	2,795
Identity Theft	27,922	Crimes Against Children	2,587
Credit Card/Check Fraud	22,985	Ransomware	2,385
BEC	21,832	Threats of Violence	2,224
Spoofing	20,649	IPR/Copyright/Counterfeit	2,183
Confidence/Romance	19,021	SIM Swap	2,026
Employment	14,946	Malware	762
Harassment/Stalking	11,779	Botnet	568
Real Estate	11,727		

*Descriptors**			
Cryptocurrency	31,310	Cryptocurrency Wallet	20,781

Source:
ic3.gov

Hodgson Russ LLP ATTORNEYS

2022 Crime Types by Victim Count

2022 CRIME TYPES continued

By Victim Loss

Crime Type	*Loss*	*Crime Type*	*Loss*
Investment	$3,311,742,206	Lottery/Sweepstakes/Inheritance	$83,602,376
BEC	$2,742,354,049	SIM Swap	$72,652,571
Tech Support	$806,551,993	Extortion	$54,335,128
Personal Data Breach	$742,438,136	Employment	$52,204,269
Confidence/Romance	$735,882,192	Phishing	$52,089,159
Data Breach	$459,321,859	Overpayment	$38,335,772
Real Estate	$396,932,821	Ransomware	*$34,353,237
Non-Payment/Non-Delivery	$281,770,073	Botnet	$17,099,378
Credit Card/Check Fraud	$264,148,905	Malware	$9,326,482
Government Impersonation	$240,553,091	Harassment/Stalking	$5,621,402
Identity Theft	$189,205,793	Threats of Violence	$4,972,099
Other	$117,686,789	IPR/Copyright/Counterfeit	$4,591,177
Spoofing	$107,926,252	Crimes Against Children	$577,464
Advanced Fee	$104,325,444		

*Descriptors***			
Cryptocurrency	$2,496,196,530	Cryptocurrency Wallet	$1,349,090,883

Source:
ic3.gov

Hodgson Russ LLP ATTORNEYS

Interaction with the FBI

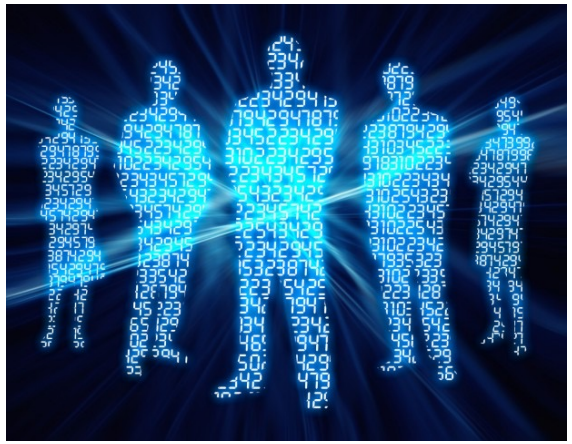
- Initial Interview or Callback by Cyber Agent:
  - Information is voluntary.
  - FBI never shares or posts information.
  - Get details and establish timeline of events.
  - Work to collect evidence, while company works to get systems back online.

Initial FBI Data Requests

- Extent of Encryption;
- Ransom Note/Letter;
- Images of Infected Machine;
- BTC Wallets;
- Emails/URLs;
- Malware Executable;
- File Extension Names.

InfraGard

InfraGard is a government and private sector alliance developed to promote the protection of the U.S. critical infrastructure.



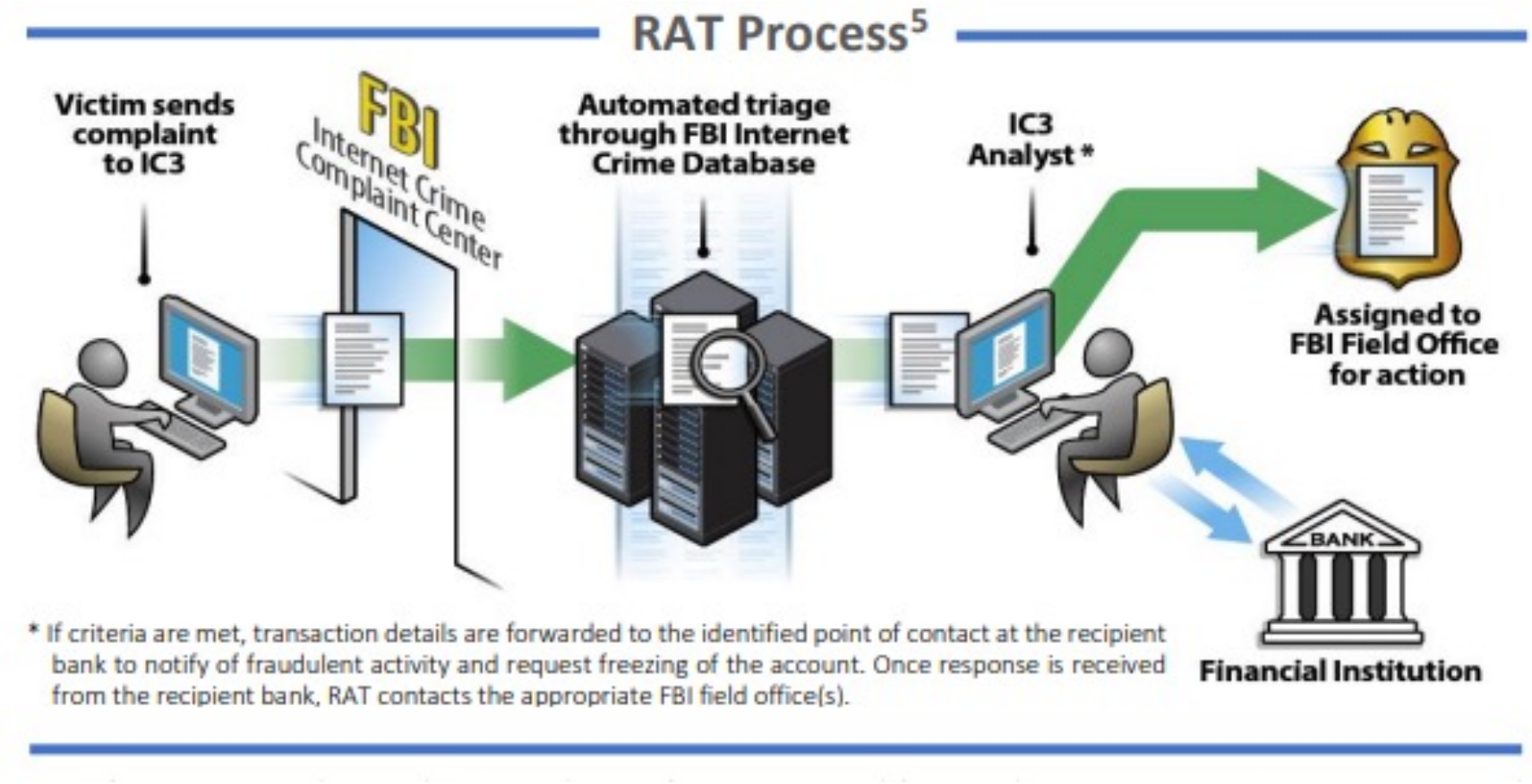
More information available at:
http://infragardbuffalo.org.

IC3: Internet Crime Complaint Center

www.ic3.gov

Source:
ic3.gov

RAT: Recovery Asset Team



Source:
ic3.gov

Recommendations for Businesses

- Conduct Security Awareness training for your employees.
- Have policies and controls to limit:
  - Access to non-work related sites (e.g. personal email, Facebook, etc…)
  - Installation of software by end-users
  - Connection of non-organizational devices to network (BYOD)
- Perform penetration testing of your systems.
- Keep your systems patched and updated.
- Keep log files.
- Offline backups. (Encryption vs. Exfiltration)
- Two-Factor/Multi-Factor Authentication.
- Have a cyber incident response plan and actively test it.
  - Have resources (internal or external) pre-identified to engage in the event of a cyber incident. After an incident occurs is not time to be trying to select a provider to assist.

CONTACT LAW ENFORCEMENT AS SOON AS IT APPEARS YOU HAVE HAD A CYBER INCIDENT.

Hodgson Russ LLP ATTORNEYS

Recommendations for Individuals

- Stay informed about common schemes and threats:
  - http://www.consumer.ftc.gov/topics/computer-security
  - http://www.ic3.gov/crimeschemes.aspx
- Keep your computer software updated – especially your web browser and associated plugins.
- Have up to date antivirus software.
- Maintain different passwords for all of your important accounts.
- Think before you click on links or attachments.
- BECs – make a phone call.

Questions?

Hodgson Russ LLP ATTORNEYS