FOLEY

FOLEY & LARDNER LLP

Data privacy, cybersecurity, and digital communication for marketing and loyalty

Aaron Tantleff

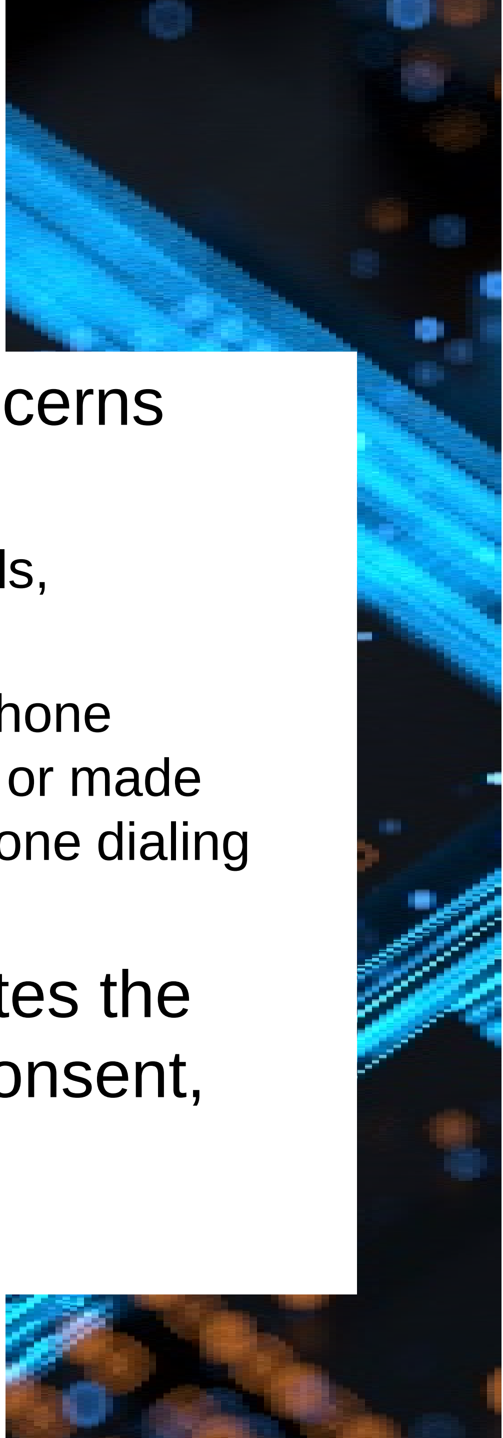
FOLEY

FOLEY & LARDNER LLP

Key Federal Privacy Laws Related to Marketing Campaigns

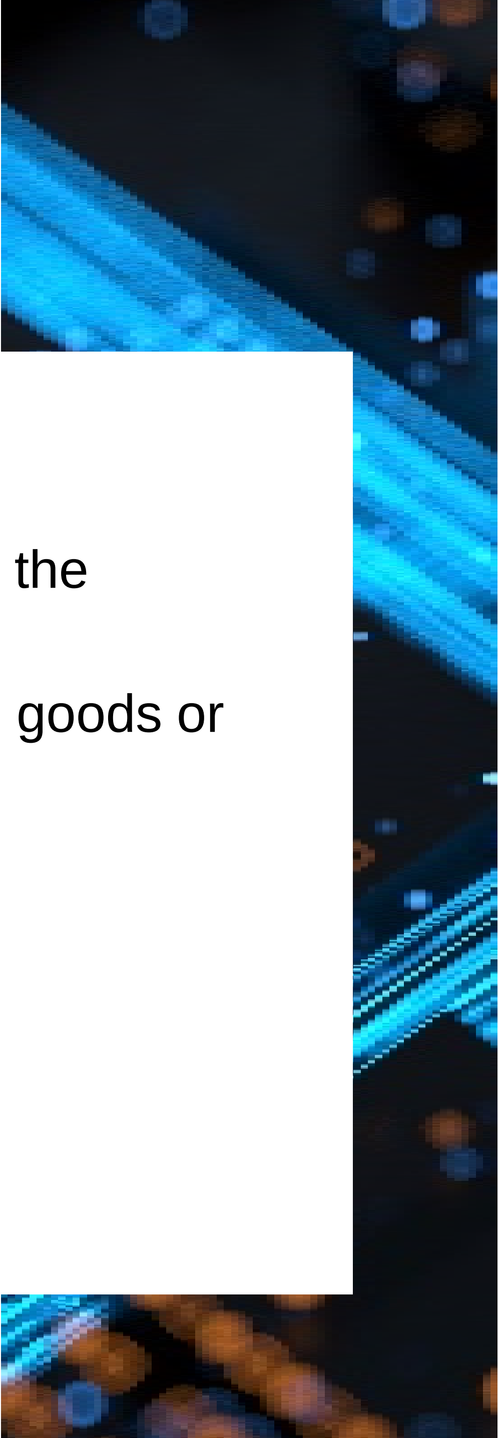
TCPA

- Enacted by Congress in 1991 to balance consumer privacy concerns against rapid increase in telemarketing
  - governs the use of automated telephone communications, such as phone calls, voicemails, faxes, and SMS
  - unlawful to “initiate” a call using an artificial or prerecorded voice to a home phone number or to “make any call (other than a call made for emergency purposes or made with the prior express consent of the called party) using any automatic telephone dialing system or an artificial or prerecorded voice.”
- A spam message is any “unsolicited advertisement” that promotes the commercially available product, good, or service without their consent, whether in writing on otherwise



TCPA

- Requirements for SMS Marketing under TCPA:
  - Wireless number call requirements apply to phone-to-phone text messages
  - Prohibits sending telemarketing texts from ATDS to any mobile phone without the consumer’s prior written consent
  - Consent not required for marketing as a condition of purchasing any property, goods or services
- Telemarketers are prohibited from contacting:
  - Residential or cellular phone lines on DNC registry
  - A consumer from whom the company has received a specific DNC request

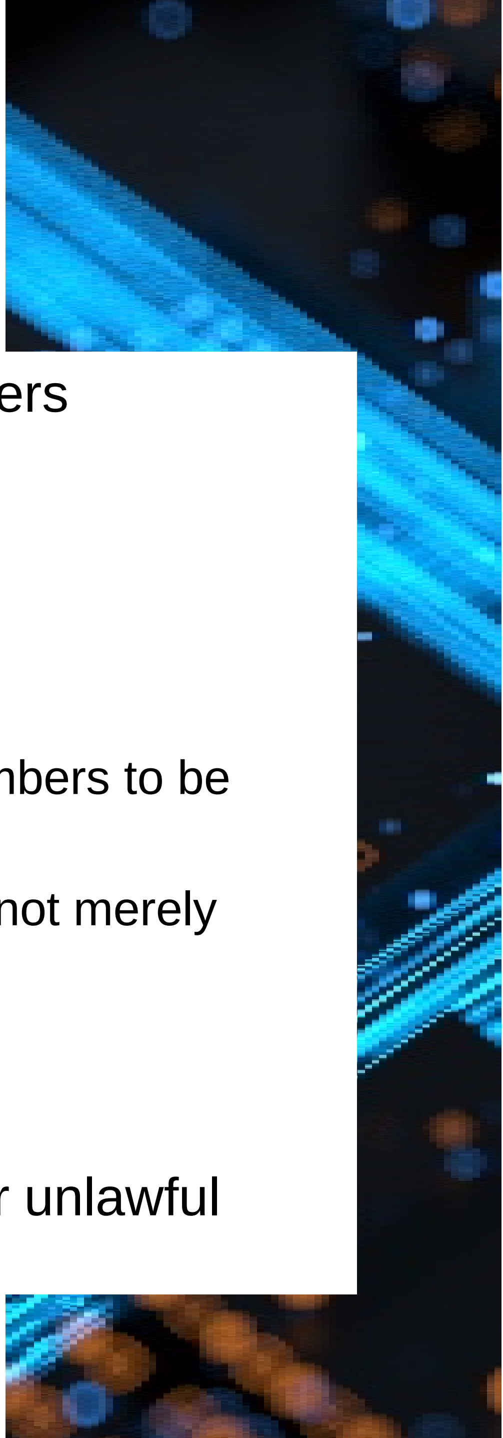


TCPA Enforcement

- Enforced by:
  - FCC
  - State AG’s or other state officials or agencies
- Private litigants may seek
  - Injunctive relief
  - Actual monetary loss or $500 in statutory damages
  - Up to three times the actual monetary loss or $1,500 in damages for each willful violation

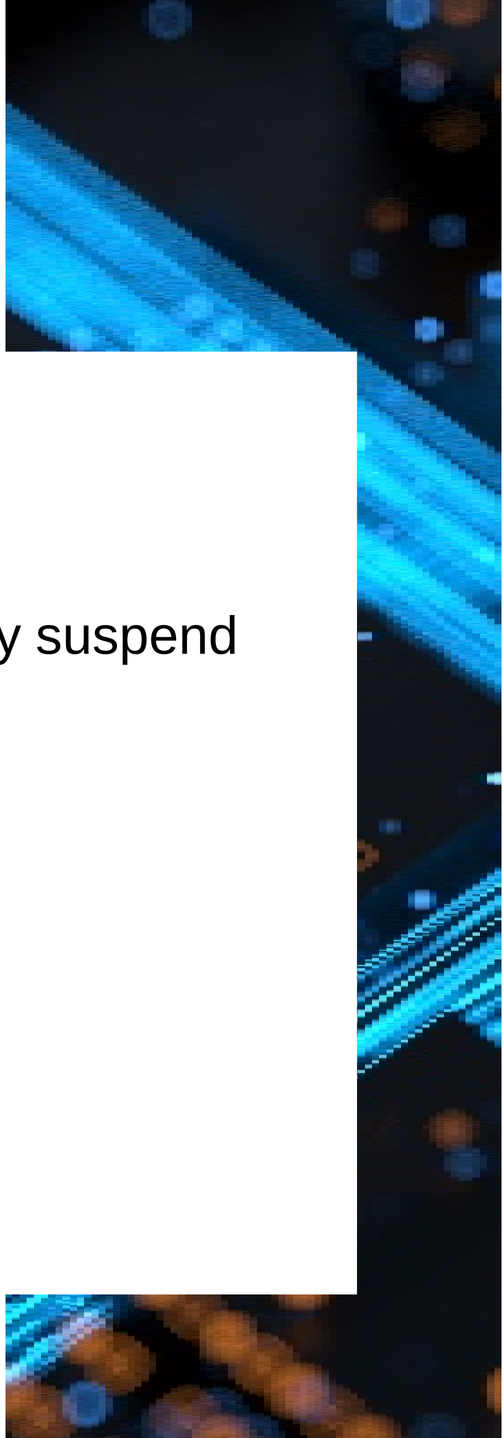
TCPA Litigation

- TCPA litigation poses risks to businesses that use texts to interact with consumers
- Interpretation of regulations constantly change
  - FCC
  - Courts
- SCOTUS clarified definition of ATDS in *Facebook Inc. v. Duguid* (2021)
  - An ATDS is equipment which has the capacity—(A) to store or produce telephone numbers to be called, using a random or sequential number generator; and (B) to dial such numbers
  - An ATDS must have the capacity to generate numbers randomly or sequentially (and not merely the ability to dial from a list of numbers) (resolving a circuit split)
- Post-*Duguid*:
  - Focus on revocation-of-consent issues into the TCPA’s do-not-call provisions
- In February 2022, FCC proposed $45M fine against health insurance agents for unlawful robocalls



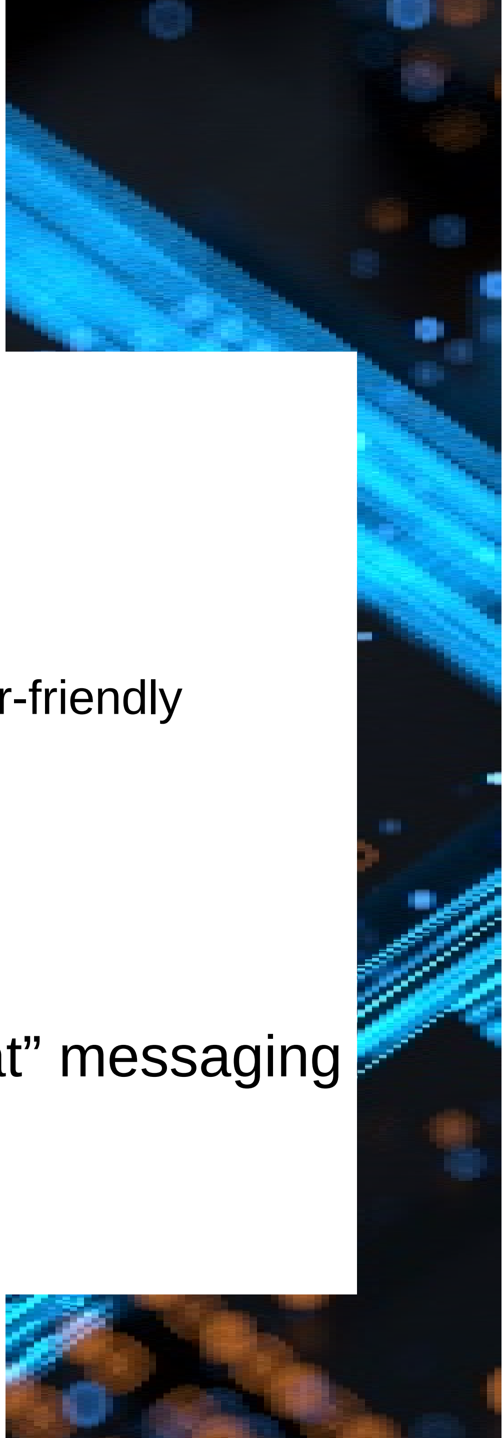
Cellular Telecommunications Industry Association (CTIA)

- Trade organizations operated by wireless companies
- Cannot be sued for disobeying CTIA guidelines
- However, violations may be reported by the CTIA to the mobile carriers and may suspend or terminate access
- Short code system
  - simple and popular method to allow people to opt-in.



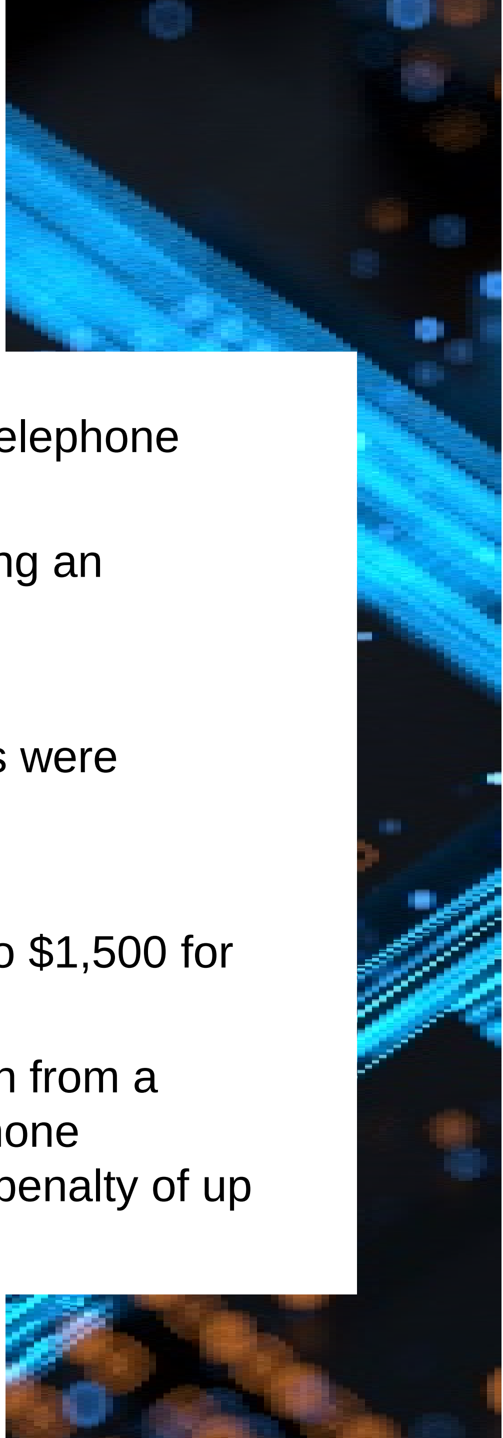
Best Practices for Complying with TCPA

- Develop a written TCPA compliance policy
  - Provide clear, accessible opt-out mechanisms
  - Establish processes for checking numbers against DNC registry
  - Process DNC and opt-out requests and establish a clear record of those requests
  - Obtain consent for telemarketing requests and informational texts in a clear, consumer-friendly manner
  - Keep informational messages free from any advertising
  - Retain records of consent for at least 4 years
  - Validate the number is legitimate by sending a text before beginning marketing efforts
- Register ads to clearly identify “who” is sending the campaign, and “what” messaging is being sent
- Keep up with State telemarketing laws



Florida Telephone Solicitation Act (FTSA)

- Expands “automated” dialer to include any “automated system for the selection or dialing of telephone numbers or the playing of a recorded message.”
- Additional restrictions including prior express written consent for all telephonic sales calls using an automated system
- Removes exemptions, including:
  - calls in response to calls initiated by persons to whom the automatic calls or live messages were directed
  - calls concerning previously ordered good or services
- Private cause of action that allows called parties to recover at least $500 per violation or up to $1,500 for willful or knowingly violating the FTSA
- Note: Texas Business and Commerce Code requires a person making a telephone solicitation from a location in Texas to hold a registration certificate with the Texas Secretary of State. If a telephone solicitation is made before registering, each violating call is a separate offense that carries a penalty of up to $5,000.

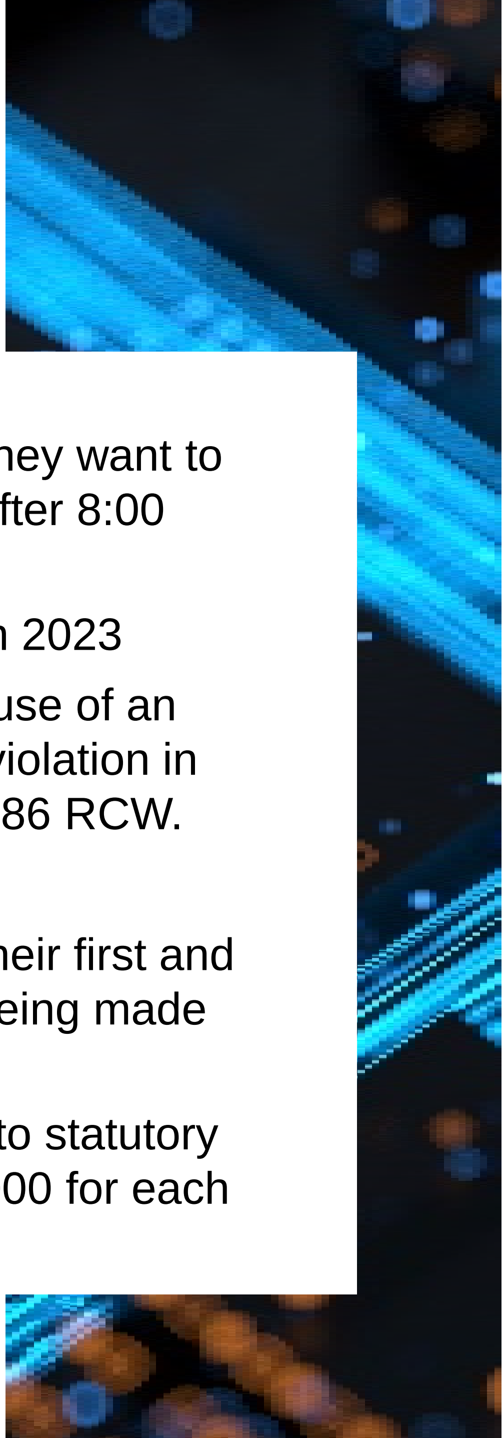


Other State Mini-TCPA Laws

- Oklahoma – House Bill 3168 (“Telephone Solicitation Act of 2022”) – *effective November 1, 2022*
  - Private right of action of at least $500 per violation
- Georgia – Senate Bill 364 (proposed amendment to Ga. Code § 46-5-27) – expected in 2023
  - Private right of action of at least $1,000 per violation
  - Includes a specific provision facilitating participation in “a class action . . . for which the damages limitation in . . . this paragraph shall not apply.”
- Washington – House Bill 1497 – *effective June 9, 2022*

Other State Mini-TCPA Laws

  - Telephone solicitor must end a call within 10 seconds if a “called party states or indicates they want to end the call” and prohibits “calls to any person which will be received before 8:00 a.m. or after 8:00 p.m. at the call recipient’s local time.”
- Washington – House Bill 1650 (proposed amendment to RCW Chapter 19.190) – expected in 2023
  - Private right of action of at least $1,000 per violation. And in the case of a violation for the use of an “automatic dialing and announcing device”, a civil litigant may recover at least $1,000 per violation in addition to all the remedies available in Washington’s consumer protection act, chapter 19.86 RCW.
- Virginia – The Virginia Telephone Privacy Protection Act
  - A telephone solicitor who makes a telephone solicitation call must identify themselves by their first and last names and the name of the person on whose behalf the telephone solicitation call is being made promptly upon making contact with the called person.
  - A failure to include both first and last names at the start of a call can exposure a company to statutory damages in the amount of $500 for a first violation, $1,000 for a second violation, and $5,000 for each subsequent violation

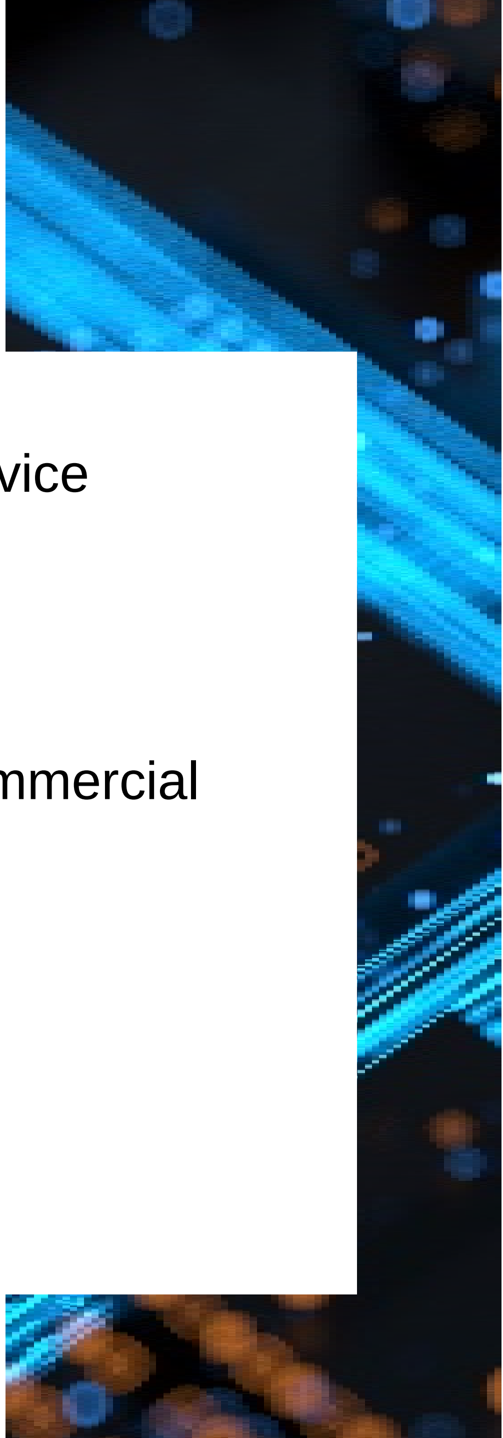


FTC’s Telemarketing Sales Rule (TSR)

- More consumer protection focused than the TCPA
  - Specific disclosure requirements
  - Does not distinguish between landline and mobile numbers
- Shared rules with TCPA
  - Pre-recorded calls to landlines
  - Do Not Call
  - Calling time restrictions
  - Automated call disclosures
- No private right of action

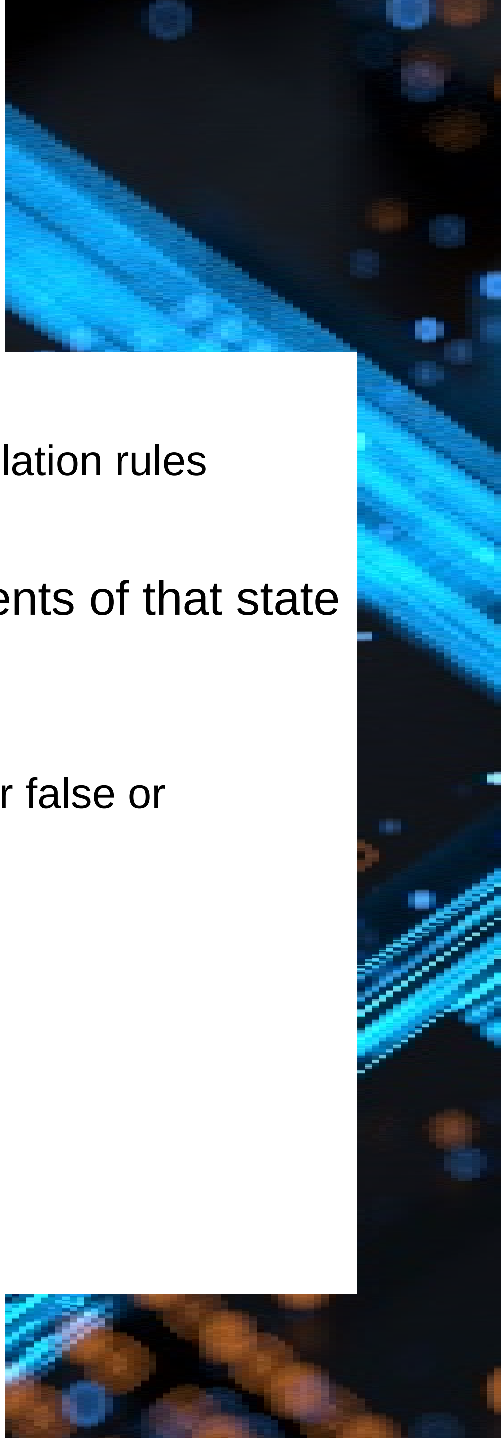
CAN-SPAM

- Enacted by Congress in 2003 to regulate unsolicited commercial email
- Applies to commercial messages used to advertise or promote a product or service
  - Email marketing
  - Internet-to-phone text messages
- Any business entity that uses commercial email messages must comply
- CAN-SPAM requires consumers prior opt-in consent to send mobile service commercial messages
- To obtain consent, the sender must
  - Clearly identify who will send the messages
  - Disclose that the wireless carrier may charge the subscriber to receive messages
  - State that the subscriber can revoke consent at any time
- Consumers have the right to opt-out



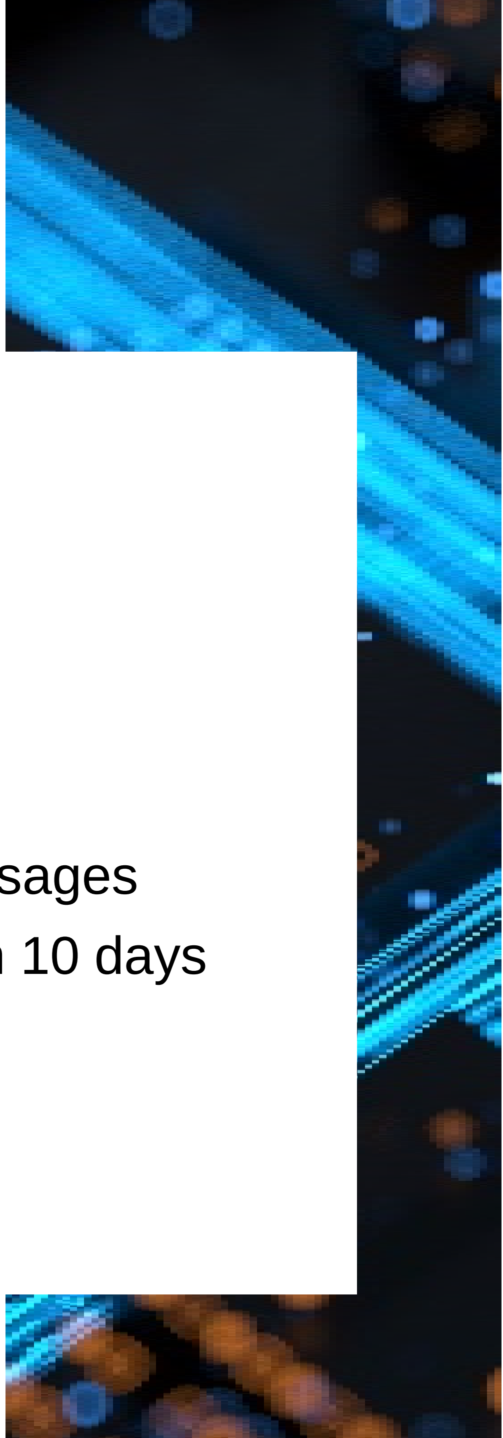
CAN-SPAM Enforcement

- Primarily enforced by the FTC
  - FTC can seek civil penalties for CAN-SPAM Act violations as if they were violations of trade regulation rules
  - Civil penalties up to $46,517 for each separate email that violates the CAN-SPAM Act
- State AGs and other regulatory agencies have power to enforce violations against residents of that state and can seek:
  - Injunctive relief
  - Damages for actual loss or statutory damages up to $250 per violation capped at $2M (claims for false or misleading information are not limited by this cap)
  - Three times the amount of statutory damages for willful, knowing, or aggravated violations
  - Costs of bringing the action and reasonable attorney fees
- Internet Service Providers may bring claims for certain violations and can seek:
  - Injunctive Relief
  - Actual damages or statutory damages up to $100 per violation capped at $1M
  - Three times the amount of statutory damages for willful, knowing, or aggravated violations



Complying with CAN-SPAM

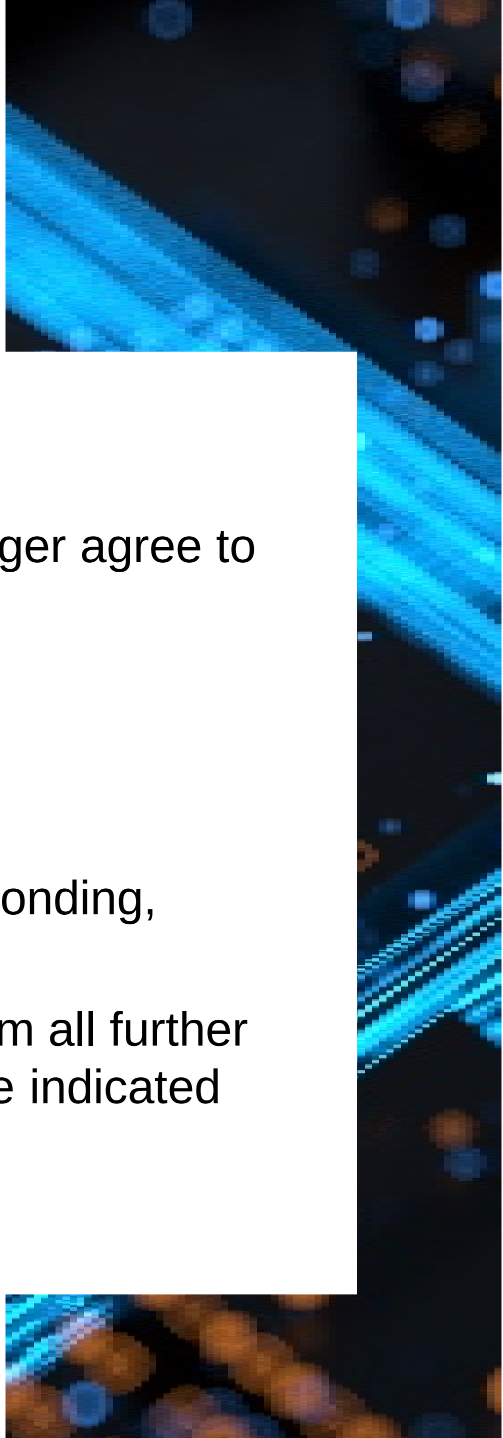
- Mailing list can only include persons who have affirmatively opted in
- Email messages cannot contain false or misleading information
- Subject line must accurately reflect content of message
- Clearly and conspicuously identify the message as an ad
- Include valid physical postal address
- Clearly and conspicuously explain how the consumer can opt-out of future messages
- Opt-out link must be valid for at least 30 days and honor opt-out requests within 10 days
- Monitor third-party vendors in control of direct marketing efforts



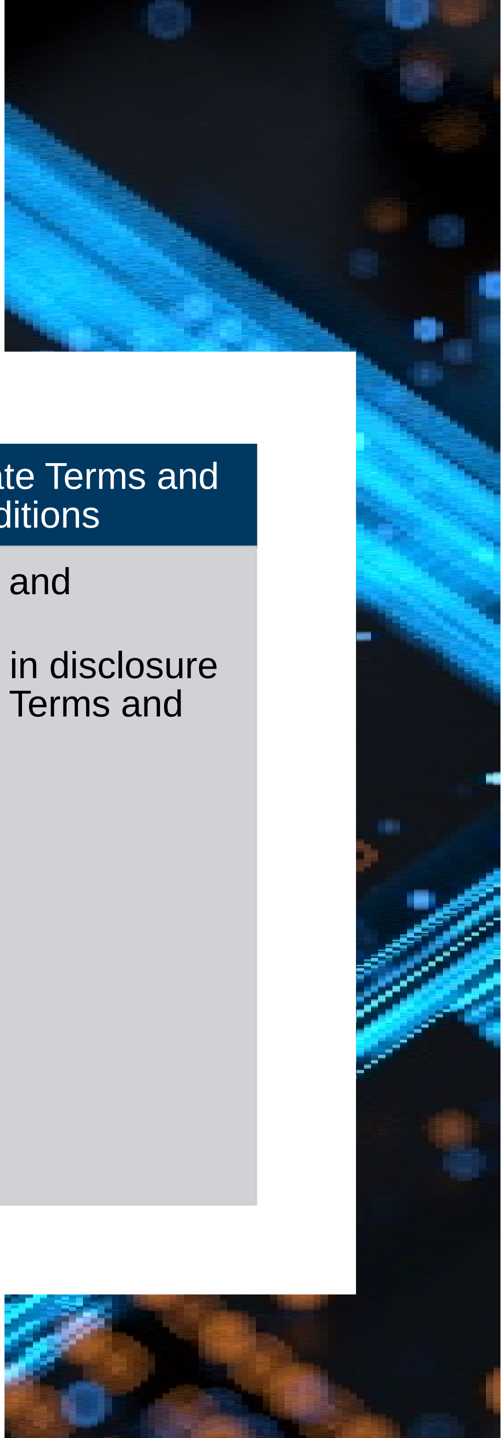
Marketing Consent

- Opt-In
  - Consumer action to enroll in program
  - Typically, consumers opt in by entering their phone number or email in a website form and selecting a box to receive exclusive offers or notifications
    - May also respond to call to actions, provide information over the phone, or via other means

- Opt-Out
  - Subscriber indicates they no longer agree to receive messages from you
  - Text Message opt out
    - Replying “STOP” to sender
  - Email opt out
    - Clicking “unsubscribe” or responding, “unsubscribe”
  - Required to remove opt-outs from all further communications, or as otherwise indicated



SMS Marketing Checklist



Explain Program at Opt-in

- Business name
- Types of messages recipients can expect
- Messaging cadence
- Std Msg&Data rates may apply
- Link to SMS terms and conditions
- Link to Privacy policy
- Opt-out instructions

Prior Express Written Consent

- Express written consent required to text consumers marketing messages
- Manually checking a box in a website form
- Verbally agreeing to opt-in (which must be recorded)
- Texting a shortcode to a designated number
- Must explicitly state that enrolling means subscribers agree to receive text messages

Confirm Opt-In

- Double opt-in
  - TCPA requires texting recipients a disclosure message confirming their participation in SMS program
  - Message reiterates the details of SMS program stated at opt-in

Communicate Terms and Conditions

- SMS Terms and Conditions
- Provide link in disclosure text to SMS Terms and Conditions

SMS Marketing Checklist

Timing	**Identify Company Name in Every Message**	Easy Opt-Out	Avoid SHAFT	Don't Message Opt-Outs
• Cannot text or call subscribers before 8:00 AM or after 9:00 PM local time		• Clear and easy for subscribers to unsubscribe • STOP		

SMS Opt-In Examples

- To receive special VacayTime deals to your mobile phone, text VACAY to 123456. You will receive a reply text msg from VacayTime verifying your enrollment, which you will need to confirm by reply text. Up to 2 automated msgs/week. Consent not required for purchase. STOP to Stop, HELP for help. Msg&DataRatesMay apply.
  - *Consumer Replies*
- Reply YES to confirm receipt of promotional automated text messages from VacayTime to this mobile number. Up to 2 automated msgs/week. Consent not required for purchase. STOP to Stop, HELP for help.

- By clicking Yes [replying to this e-mail], I consent to receive phone calls from VacayTime, regarding VacayTime's properties, at the phone number above, including my wireless number if provided. I understand these calls may be generated using an automated technology and that my consent is not required to make a purchase.

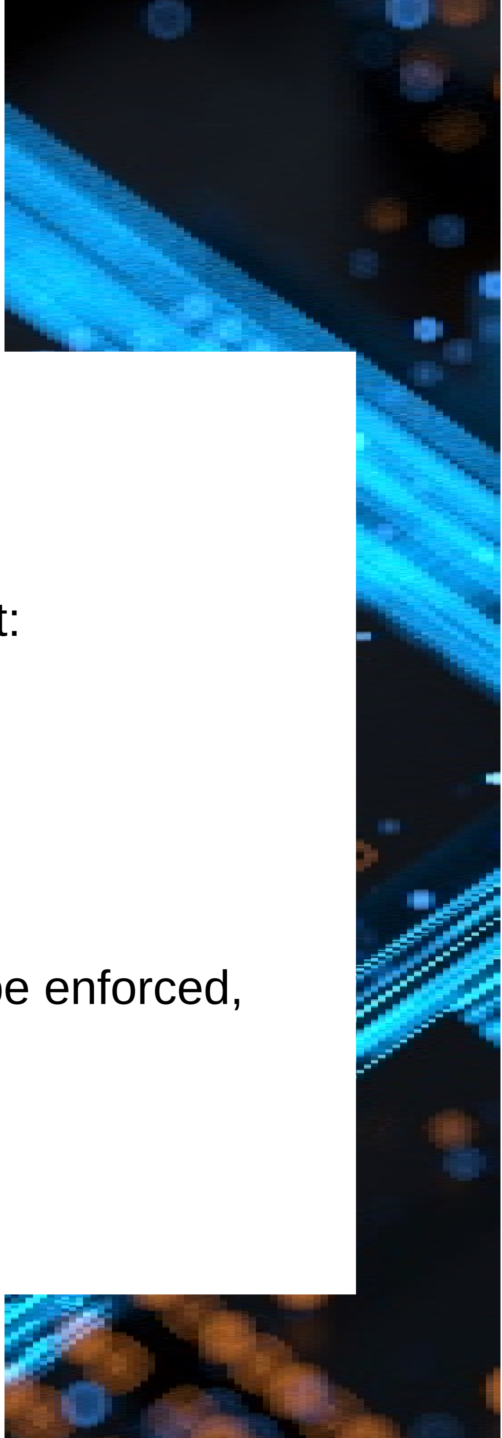
FOLEY

FOLEY & LARDNER LLP

Brief Overview of U.S. Privacy Laws

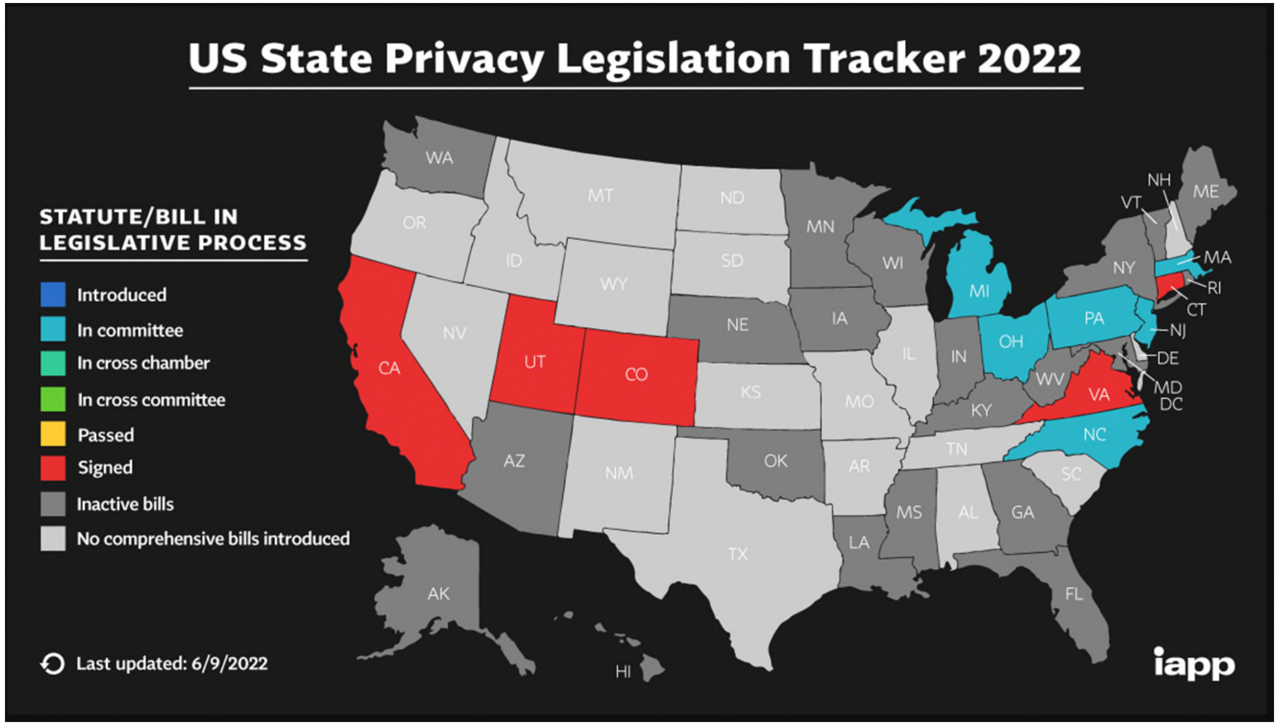
Overview of State General Privacy Laws

- Only California has a comprehensive privacy law that is currently in effect
  - California Consumer Privacy Act (CCPA)
- Four states, including California, have comprehensive privacy laws soon to go into effect:
  - California: California Privacy Rights Act (CPRA) - *effective 1/1/2023*
    - fully enforceable on 7/1/2023
    - look-back period to 1/1/2022
  - Colorado: Colorado Privacy Act - *effective 7/1/2023*
    - AG may adopt rules before 1/1/2025 that may further change the law or how it will be enforced, which would become effective by 7/1/2025
  - Virginia: Consumer Data Protect Act - *effective 1/1/2023*
  - Connecticut: Consumer Data Privacy Act - *effective 1/1/2023*



States Considering Privacy Statutes

- 21 states have introduced some form of privacy related legislation in 2021, some have renewed efforts, some are in committee
- More laws and regulations will increase cost of doing business and make it more complex for companies to comply
- Regulations based on consumer residence, not company headquarters or principal place of business



US State Privacy Legislation Tracker 2022

Last updated: 6/9/2022

Common Principles Across Existing Data Privacy Laws

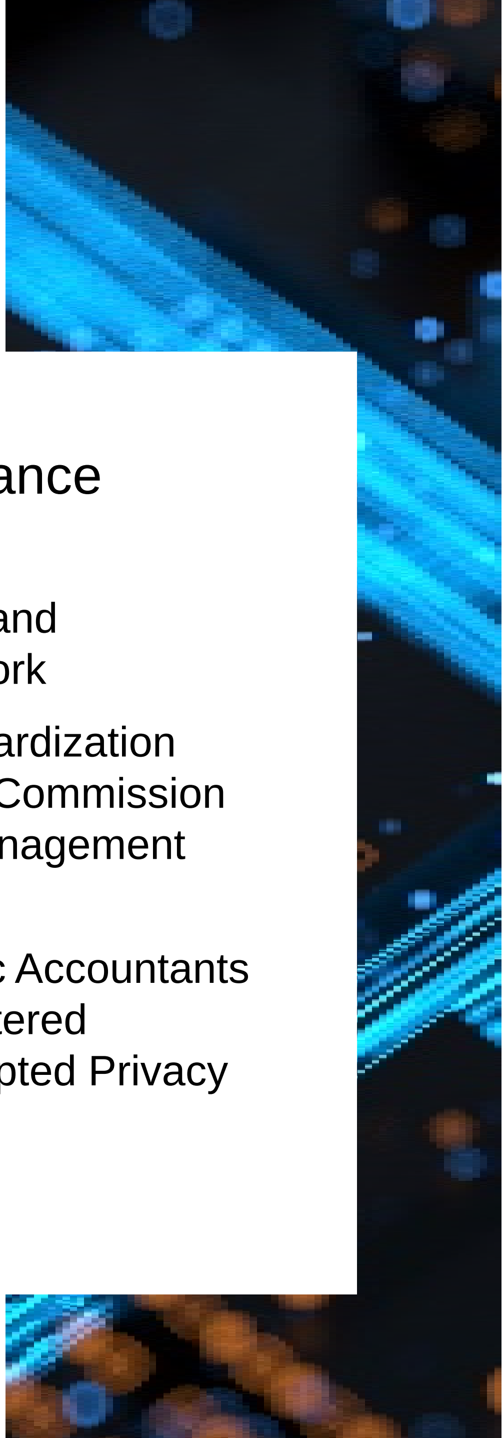
- Scope/applicability/exemptions
- Individual rights – e.g., access, rectification, deletion, restriction, portability, opt-out
- Notice/transparency requirements
- Legal basis for processing
- Processing principles – e.g., purpose limitation and data minimization

- Vendor requirements
- Data breach notification
- Security requirements
- Recordkeeping
- Risk/impact assessments
- International data transfer restrictions

Tips for Developing a Privacy Compliance Program

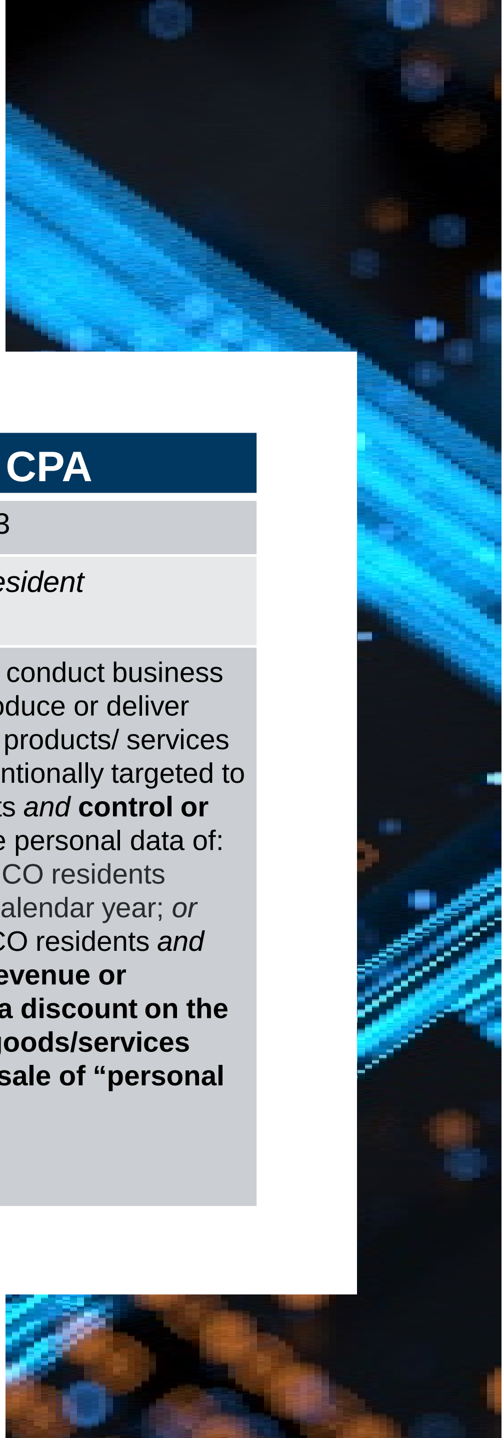
- Data mapping
- Performing a risk assessment
- Determining legal and program requirements
- Developing policies/internal controls
- Managing vendor privacy compliance

- Implementing a privacy compliance framework
  - The National Institute of Standards and Technology (NIST) Privacy Framework
  - International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27701 Privacy Information Management Systems
  - American Institute of Certified Public Accountants (AICPA)/ Canadian Institute of Chartered Accountants (CICA) Generally Accepted Privacy Principles (GAPP)



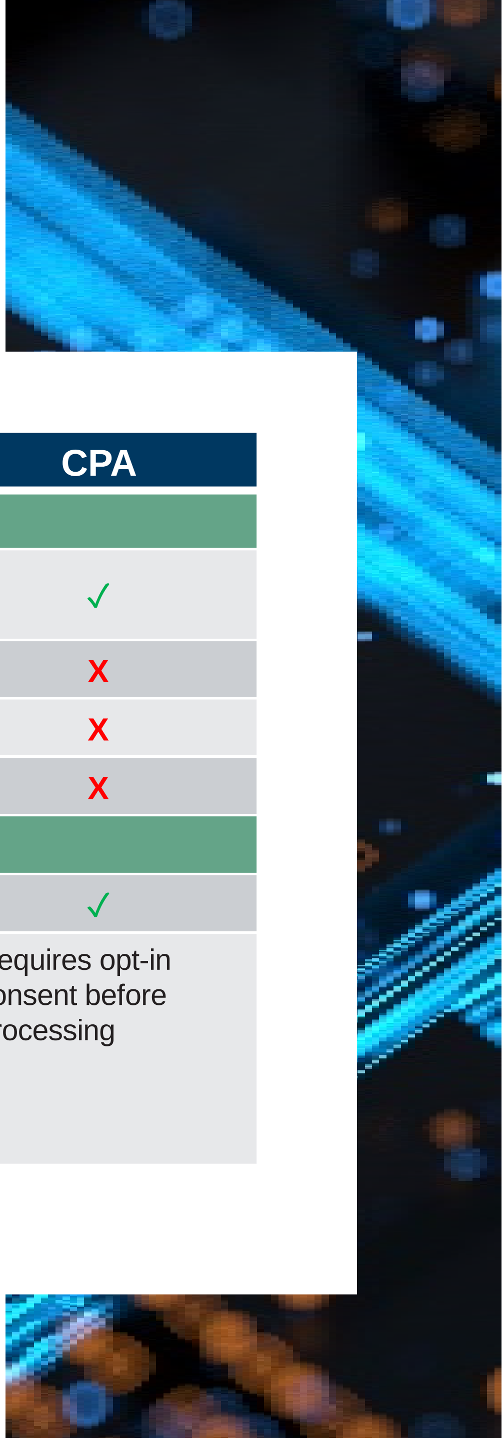
European and U.S. Privacy Laws: The Basics

	GDPR	CCPA	CPRA	VCDPA	CPA
Effective	May 25, 2018	January 1, 2020	January 1, 2023	January 1, 2023	July 1, 2023
Protected individuals	Person *in* the EU	California *resident*	California *resident*	Virginia *resident*	Colorado *resident*
Regulated entities	Entities that are: ▪ **Established in the EU** and process “personal data” as part of its EU establishment’s activities; *or* ▪ Established outside the EU **and offer goods or services to, or monitor the behavior of, individuals in the EU**.	For-profit entities that do business in CA *and*: ▪ Have **annual gross revenues in excess of $25M**; *or* ▪ Annually buys, receives, sells, or shares “personal information” of **≥50,000** CA residents, households, or devices; *or* ▪ Derives **50% or more of its annual revenues from selling** CA residents’ “personal information”	For-profit entities that do business in CA *and*: ▪ Had **annual gross revenues in excess of $25M in the preceding calendar year**; *or* ▪ Annually buys, sells, or shares “personal information” of **≥100,000** CA residents or households; *or* ▪ Derives **50% or more of annual revenue from selling or sharing** CA residents’ “personal information.”	For-profit entities that conduct business in VA *or* produce or deliver products/services that are targeted to VA residents *and* **control or process** the “personal data” of: ▪ **≥100,000** VA residents during a calendar year; *or* ▪ **≥25,000** VA residents *and* **derive more than 50% of gross revenue from the sale of “personal data.”**	Entities that conduct business in CO *or* produce or deliver commercial products/ services that are intentionally targeted to CO residents *and* **control or process** the personal data of: ▪ **≥100,000** CO residents during a calendar year; *or* ▪ **≥25,000** CO residents *and* **derives revenue or receives a discount on the price of goods/services from the sale of “personal data.”**



European and U.S. Privacy Laws: Protected Data

	GDPR	CCPA	CPRA	VCDPA	CPA
Protected data generally					
Broad definition of "personal data" or "personal information"	✓	✓	✓	✓	✓
Includes publicly available data	✓	X	X	X	X
Includes B2B data	✓	X	✓	X	X
Includes employment data	✓	X	✓	X	X
Sensitive data					
Defined category	✓	X	✓	✓	✓
Heightened protections	▪ Processing prohibited unless a GDPR Article 9 condition is met	N/A	▪ Purpose limitations for collection & use ▪ Consumers have a right to limit use & disclosure	▪ Requires opt-in consent for processing	▪ Requires opt-in consent before processing

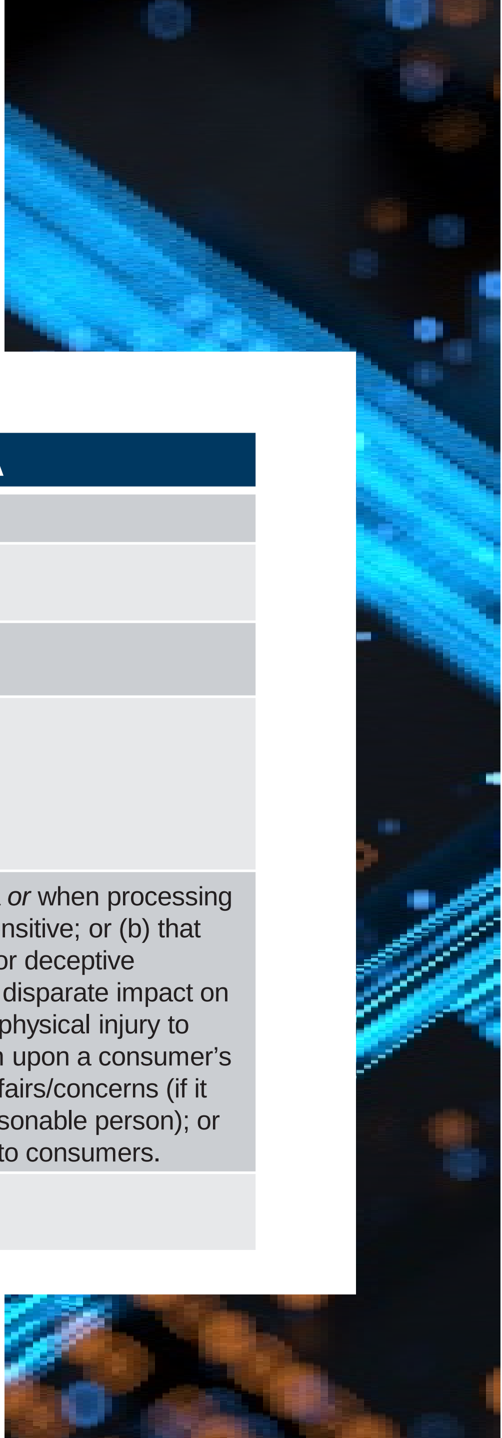


European and U.S. Privacy Laws: Consumer Rights

	GDPR	CCPA	CPRA	VCDPA	CPA
Right to know/access	✓	✓	✓	✓	✓
Right to data portability	✓	✓	✓	✓	✓
Right to delete	✓	✓	✓	✓	✓
Right to correct	✓	X	✓	✓	✓
Right to limit use of data	✓	X	✓ (sensitive PI only)	X	X
Right to opt-out of sale	✓ (implied)	✓	✓	✓	✓
Right to opt-out of “sharing” or processing for “targeted advertising”	✓ (implied)	X	✓	✓	✓
Right to opt-out of or object to automated decision making	✓	X	✓	✓	✓
Right to non-discrimination	✓ (implied)	✓	✓	✓	✓

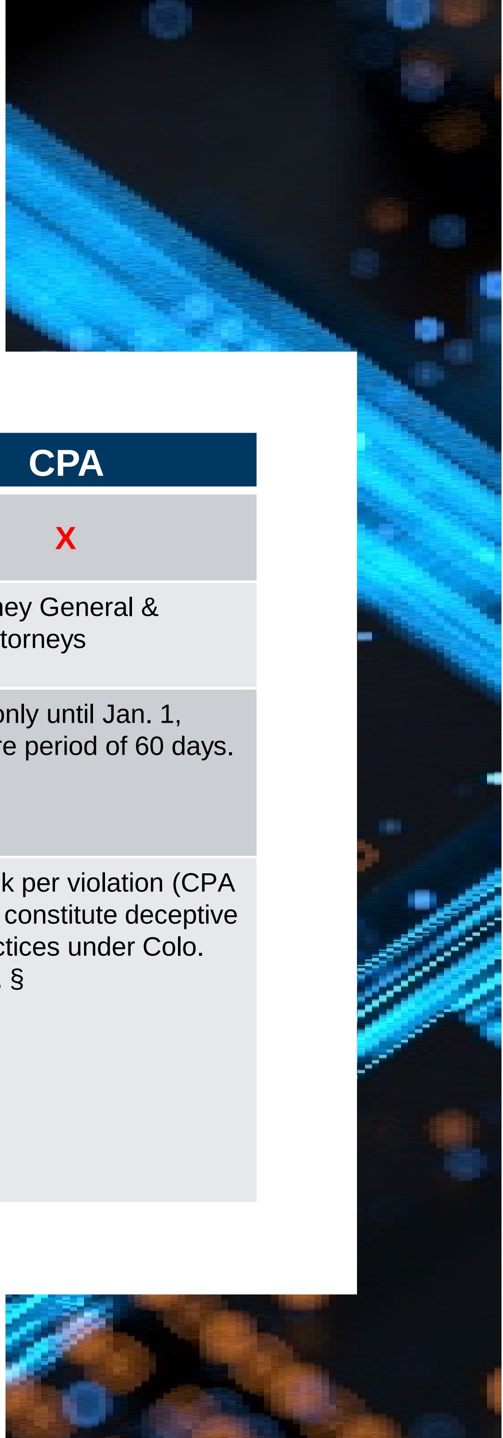
European and U.S. Privacy Laws: Business Obligations

	GDPR	CCPA	CPRA	VCDPA	CPA
Be transparent	✓	✓	✓	✓	✓
Specify purpose for collection/processing	✓	✓	✓	✓	✓
Minimize data collection	✓	X	✓	✓	✓
Obtain opt-in consent for processing	When consent is the lawful basis for processing	For minors; those who have previously opted-out; and upon entry into a financial incentive program	For minors; those who have previously opted-out; and upon entry into a financial incentive program	For sensitive data	For sensitive data
Conduct risk assessments	When processing is likely to result in a high risk to the rights & freedoms of natural persons	X	When processing presents significant risk to consumers' privacy or security	When selling personal data *or* when processing personal data: (a) that is sensitive; (b) for targeted advertising / profiling; or (c) that presents a heightened risk of harm to consumers	When selling personal data *or* when processing personal data: (a) that is sensitive; or (b) that presents a risk of (i) unfair or deceptive treatment of, or unlawful or disparate impact on consumers; (ii) financial or physical injury to consumers; (iii) an intrusion upon a consumer's seclusion or their private affairs/concerns (if it would be offensive to a reasonable person); or (iv) other substantial injury to consumers.
Implement data security practices	✓	✓	✓	✓	✓



European and U.S. Privacy Laws: Enforcement

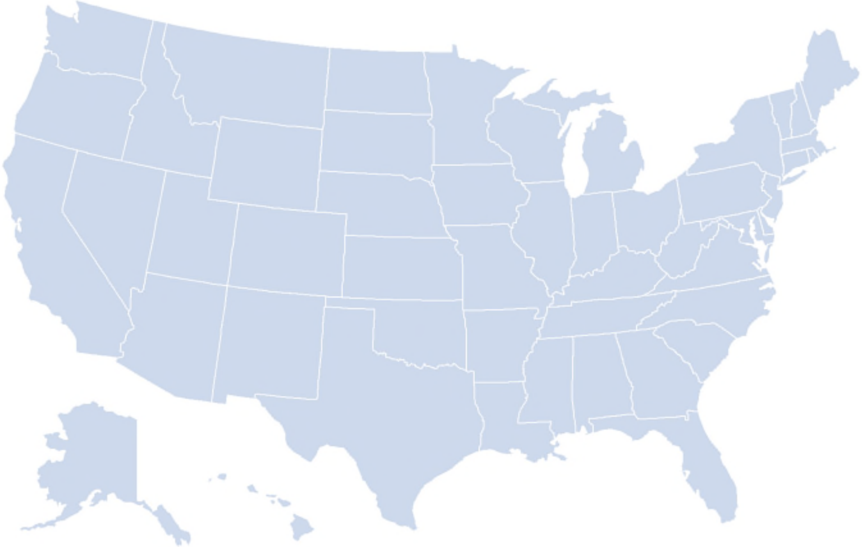
	GDPR	CCPA	CPRA	VCDPA	CPA
Private right of action	✓	Only for security breaches	Only for security breaches	X	X
Regulatory authority	EU Supervisory Authorities	CA Attorney General	CA Attorney General & CA Privacy Protection Agency (CPPA)	VA Attorney General	CO Attorney General & District Attorneys
Opportunity to cure violations	X	Yes, for actions brought by consumers and the AG. Cure period of 30 days.	Yes, but in the context of administrative actions, only at the CPPA's discretion. 30 day cure period for consumer actions only.	Yes, cure period of 30 days.	Yes, but only until Jan. 1, 2025. Cure period of 60 days.
Fines for violations	Up to €20 million or 4% of total worldwide revenue	▪ Consumers: actual damages or up to $750 per consumer per incident ▪ AG: up to $2.5k/$7.5k per unintentional/ intentional violation	▪ Consumers: actual damages or up to $750 per consumer per incident ▪ AG/CPPA: up to $2.5k/$7.5k per unintentional/intentional violation (or each violation involving the personal information of minor consumers)	Up to $7.5k per violation	Up to $20k per violation (CPA violations constitute deceptive trade practices under Colo. Rev. Stat. § 6-1-112)



Cyber Threat Landscape Overview

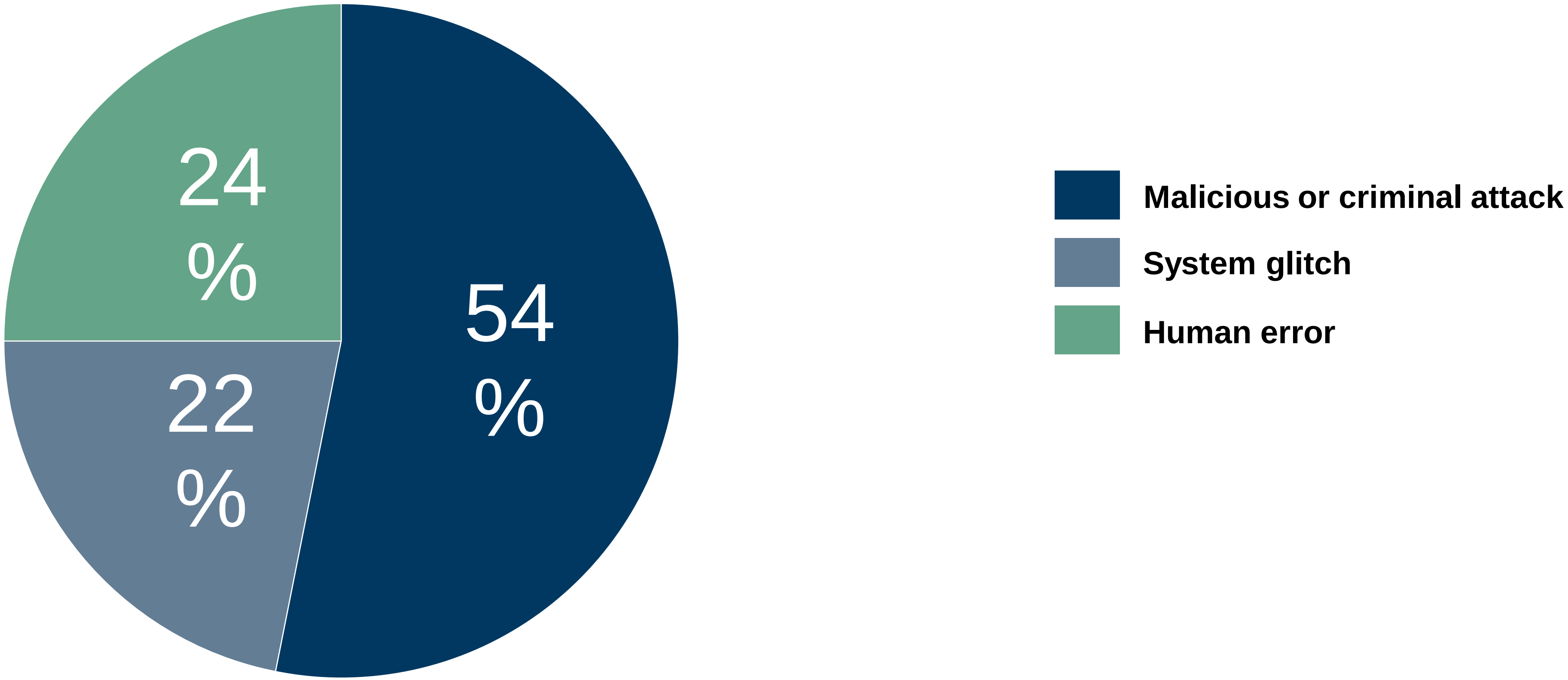
Cost Overview

- Average Cost of a U.S. Data Breach: $9.05 million
  - Has increased 244% in the past 15 years
  - Global average is $4.24 million
  - 10% increase in average cost of a breach from 2020-2021
- Cost of a breach can include detection and escalation, notification, ex-post response, and lost business records



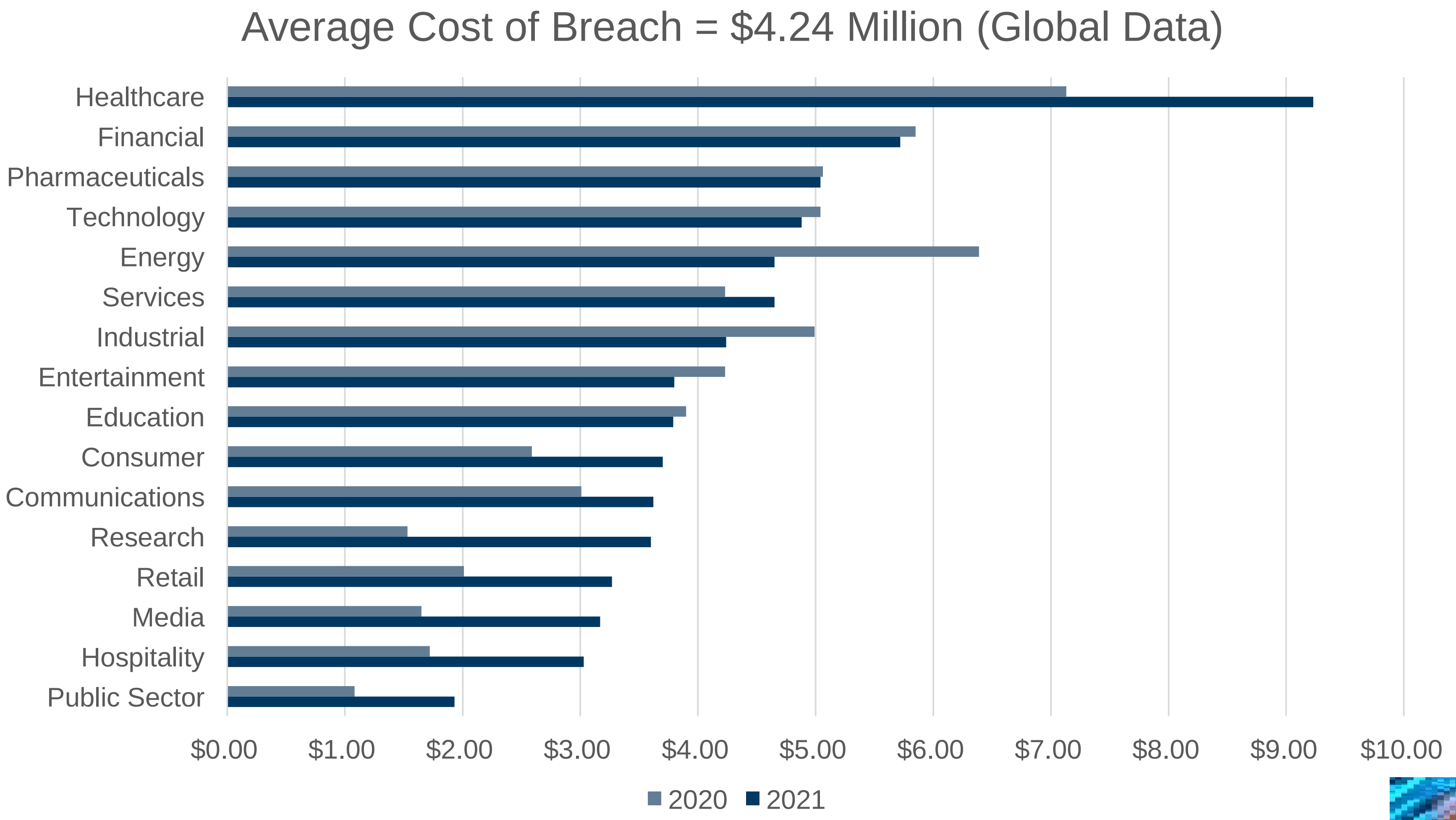
Source: Ponemon Institute© Research Report (sponsored by IBM Security),
2021 Cost of a Data Breach: United States **(August 2021)**

Sources of Risk

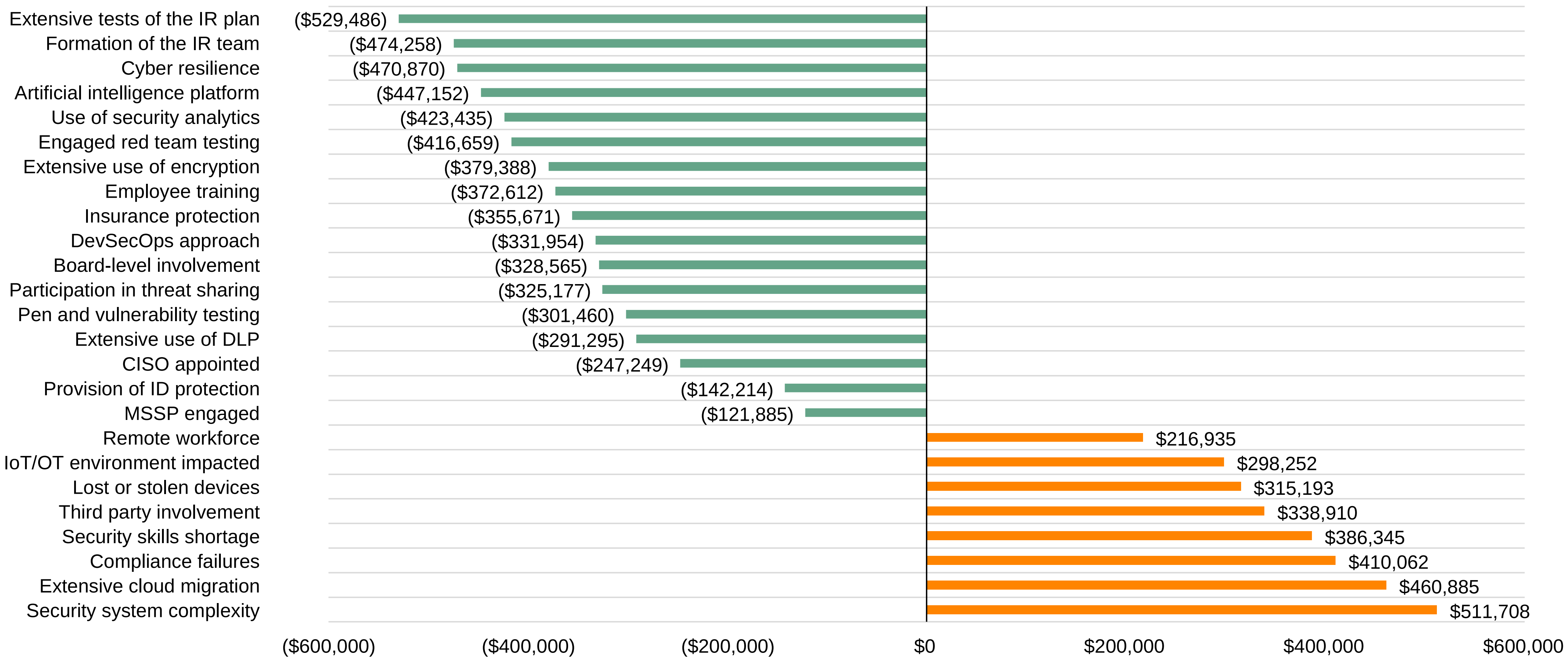


Source: Ponemon Institute© Research Report (sponsored by IBM Security), *2020 Cost of a Data Breach: United States* (October 2020)

Cost Varies by Industry



Impact of 25 Factors on the Per Capita Cost of a Data Breach



Source: Ponemon Institute© Research Report (sponsored by IBM Security),
2020 Cost of a Data Breach: United States **(October 2020)**

Source of Potential Liability & Costs for Inadequate Security Measures

- FTC and Other Applicable Industry-Specific Agency Enforcement
- State Attorney General/Other Consumer Protection Agencies Enforcement
- Class Action and Other Lawsuits
- Contractual Liability
- Data Breach Remediation and Related Costs
- Reputational Costs
- Loss of Competitive Advantage/Profits
- Ransom Payments
- International Data Protection Authorities (fines)

FOLEY
FOLEY & LARDNER LLP

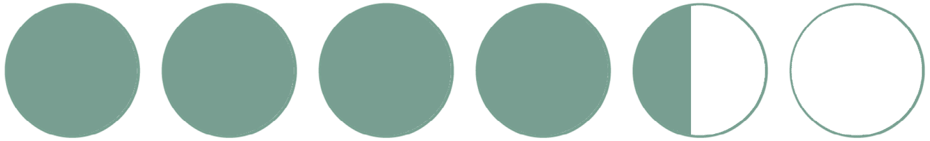
Ransomware

Rise of Ransomware

- Ransomware by the numbers
  - Ransomware attacks increased **105%** in 2021[1]
  - 2021 saw an estimated 623.3 million attempted ransomware attacks[2]
  - Globally, ransomware attacks ($4.62M) cost more than the average data breach ($4.24M)[3]

[1] 2022 SonicWall Cyber Threat Report
[2] 2022 SonicWall Cyber Threat Report
[3] Ponemon Institute© Research Report (sponsored by IBM Security), 2021 Cost of a Data Breach Report (August 2021)

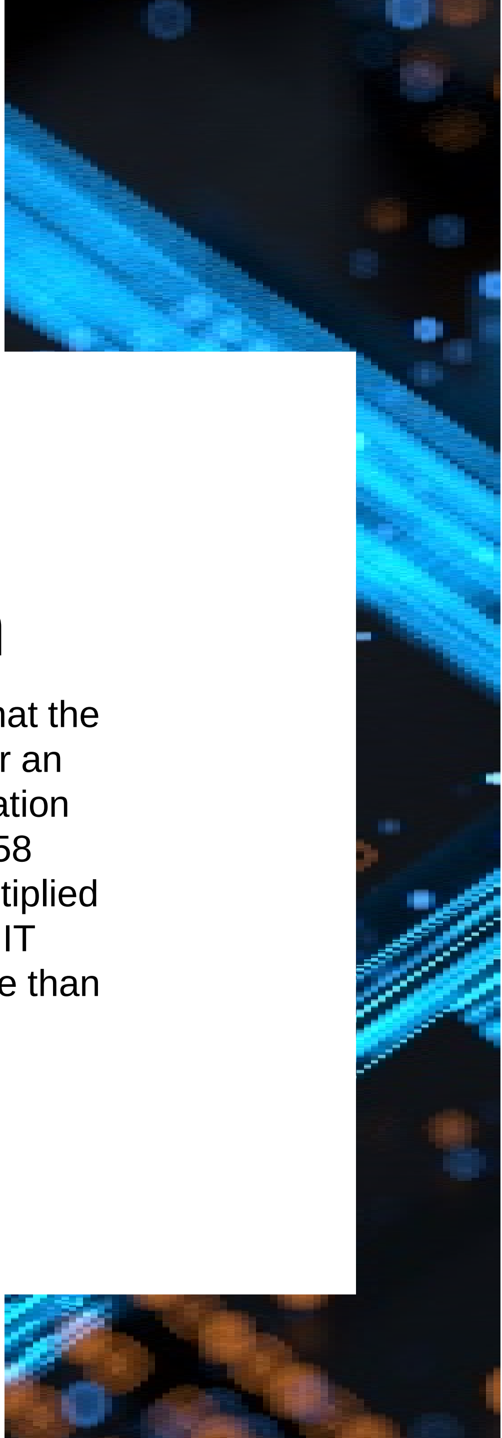
Costs Beyond Ransom Payment



32,258 hours

$2 million

Proofpoint has found that the remediation process for an average-sized organization takes on average 32,258 hours, which when multiplied by the average $63.50 IT hourly wage totals more than $2 million.



Costs Beyond Ransom Payment

- Losses Associated with Company Downtime
- Loss of Current Customers
- Negative Press & Damage to Brand
  - Loss of Future Customers
  - Loss of Investment
- Data Breach Notification
  - Cost of mailing letters
- Legal Fees
- IT Costs
  - Issue Discovery
  - Remediation
  - Operations Recovery
- Vendor Costs
  - Computer Forensics
  - Penetration Testing
- Regulatory Fines

Adjusting Your Compliance Program to Changing Regulatory Enforcement Risks

- Follow the latest guidance from the White House
  - Federal guidance frequently becomes a defacto standard
- Keep up with latest enforcement trends specific to your industry
  - FTC, Attorneys General, OCR/HIPAA, Insurance Commissioners
- Do not pay or promise to pay ransom to any sanctioned persons, groups, or regions
  - Individuals or entities on OFAC’s Specially Designated Nationals and Blocked Persons List
  - Individuals or entities covered by comprehensive country or region embargoes
    - (e.g., Cuba, the Crimea region of Ukraine, Iran, North Korea, and Syria)
- Minimize risk of costly enforcement actions by maintaining excellent cybersecurity posture
  - Implement, update, and enforce thorough cybersecurity policies and procedures
  - Ensure all cybersecurity practices meet or exceed industry standard
    - This includes keeping systems and infrastructure updated, patching all known vulnerabilities, multi-factor authentication, and training staff on phishing and cybersecurity awareness