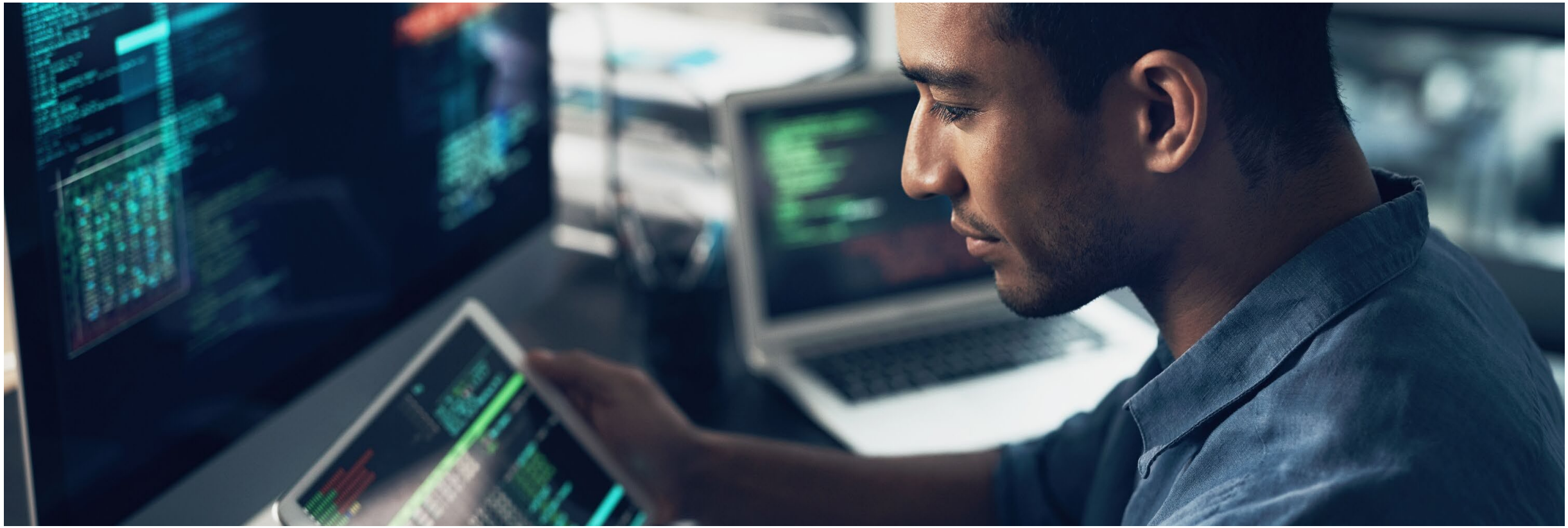


# Identify Privacy Risks Beyond Traditional Frameworks
## **IT Risk & Compliance – *Sensitive Data***

January 21, 2026

forvis mazars

# Meet Your Presenters

**Nikole Davenport, JD, LLM, CIPP-US, CIPM, FIP**

Director, Privacy

**Diana Ramirez, MHA, CHC, CHPC**

Manager, HIPAA

**Darin McLaury**

Director, IT Risk & Compliance

# Learning Objectives

1. Awareness of the intersections and gaps between Federal and State privacy laws

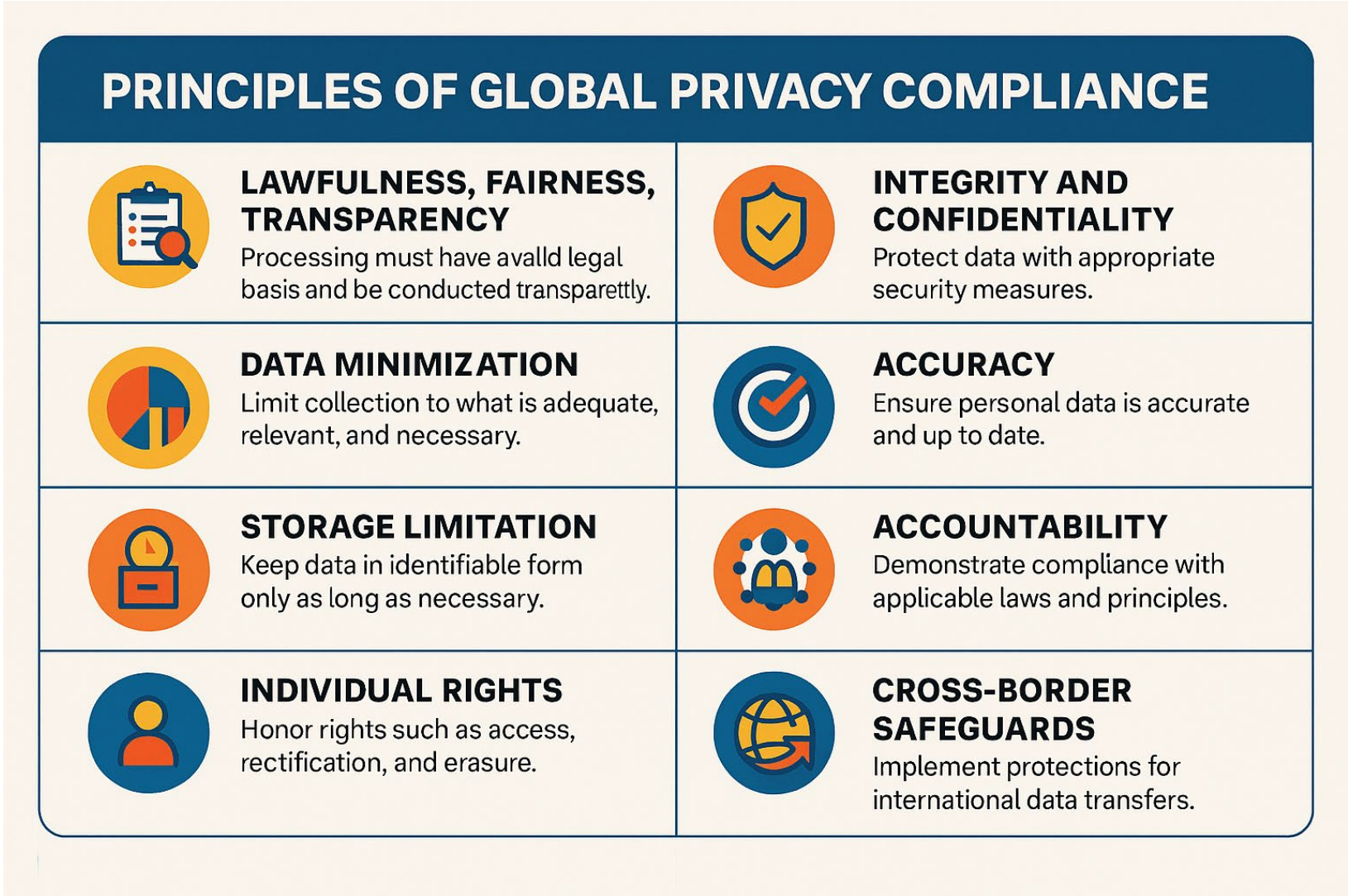
2. Overview of emerging regulations that may present compliance mandates beyond traditional sectoral frameworks

3. Understanding regulatory enforcement risks related to personal information, including health and financial data

# 01

## Privacy Regulations & Enforcement

# Good Privacy Hygiene



# 7 THINGS TO KNOW BEFORE CCPA UPDATES TAKE EFFECT

New California Consumer Privacy Act regulations go into effect January 1, 2026

## 1. Risk Assessments

Businesses must conduct a risk assessment before starting several activities, like processing sensitive personal information, selling/sharing personal information, and using or training certain automated technologies.

## 2. Requests to Opt-out of Selling/Sharing

Businesses must provide a way for consumers to confirm the status of their opt-out request, including requests submitted through opt-out preference signals.

## 3. Requests to Know

Businesses that keep personal information longer than 12 months must allow consumers to request to access all their information going back to January 2022.

## 4. Requests to Correct

Businesses must now inform consumers of their source of the inaccurate information or inform the source of the inaccuracy themselves.

## 5. Maintaining Correct Data

Businesses must make sure information that has been corrected is not overridden by inaccurate information later received, such as from data brokers.

## 6. Health Data Corrections

In certain circumstances and at the consumer's request, businesses must disclose the consumer's statement contesting the accuracy of their health information.

## 7. Sensitivity of Youth Data

The personal information of consumers under 16 years old is now considered sensitive personal information, and its use may be subject to a request to limit.

https://cppa.ca.gov/regulations/
https://cppa.ca.gov/about_us/contact.html

CalPrivacy

INDIANA CONSUMER DATA PROTECTION ACT

## DATA CONSUMER BILL OF RIGHTS

### II. Indiana Consumer Data Protection Bill of Rights.

This Consumer Bill of Rights is a summary of your rights as an Indiana resident under the Indiana Consumer Data Protection Act ("CDPA"). *Under the CDPA, a "controller" is the person or entity that collects your personal data and determines how it is processed.*

1. You have the right to obtain confirmation from a controller as to whether your personal data is being processed by the controller.
2. You have the right to obtain — once a year, free of charge — a copy or representative summary of the personal data you previously provided to a controller.
3. You have the right to correct inaccuracies in the personal data you previously provided to a controller.
4. You have the right to have your personal data deleted by a controller.
5. You have the right to opt out of a controller processing your personal data for targeted advertising, the sale of your personal data, and profiling.
6. You have the right to receive your personal data from a controller in a readily usable format so you can transfer it without hindrance.
7. You have the right to appeal a controller's denial of your request to exercise your rights under the CDPA.
8. You have the right not to be discriminated against by a controller for exercising your consumer rights under the CDPA.
9. You have the right to have your personal data processed by a controller in accordance with state and federal laws that prohibit unlawful discrimination against consumers.

INDIANA CONSUMER DATA PROTECTION ACT

DATA CONSUMER BILL OF RIGHTS

10. You have the right to exercise these consumer rights on behalf of your children.
11. You have the right to expect that your children's data will not be processed by a controller without your consent.
12. You have the right to expect that your sensitive data will not be processed by a controller without your consent, including information that reveals your racial or ethnic origin, religious beliefs, mental or physical health diagnoses, sexual orientation, citizenship, immigration status, identifying genetic or biometric data, and precise geolocation data.
13. You have the right to know a controller's data processing activities. A controller must provide a reasonably accessible, clear and meaningful privacy notice detailing the categories of personal data being processed, the purpose of the processing, the categories of personal data being shared with third parties, and the categories of third parties with whom personal data is being shared.
14. You have the right to have the collection of your personal data limited to what is adequate, relevant and reasonably necessary to the purpose communicated to you by the controller.
15. You have the right to expect that your personal data will not be used for purposes that are neither reasonably necessary for nor compatible with the purposes communicated to you by a controller, unless the controller obtains your consent.

Sources:
https://cppa.ca.gov/about_us/contact.html
https://www.in.gov/attorneygeneral/files/Indiana-Consumer-Data-Protection-Consumer-Bill-of-Rights_Web.pdf



forvis mazars

# Differences in State Laws

## Sensitive Data Definition

**Not Universal**

- **CT, DE, NJ, MD** include Gender, Financial, Pregnancy, & Health data
- **CA** adds precise geolocation, racial/ethnic origin, & union membership
- **MD** expands to include biometric & neural data

## Notice & Consent Models

- **Opt-Out Model:** Most states (*e.g.*, VA, CO, TX) follow this
- **Opt-In for Sensitive Data:** Required in CA, CT, CO, MD, & others
- **Strict Consent:** Maryland & Oregon require explicit consent for certain processing activities

## Children's Data Protections

- **CT, CA, OR, MT, NH, MN, NJ, DE, VA:** Require opt-in for targeted ads for ages 13–18
- **MD:** Bans targeted advertising for ages 13–17
- **NY:** Enacted a unique Child Data Protection Act with age-flagging requirements
- **LA, UT, TX** requires notice of age signals for apps

## AI & Automated Decision Making

- **CO** passed the first AI law in U.S. focusing on transparency & consumer protection
- **CA & MD:** Require disclosures & opt-outs for automated profiling
- **Emerging Trend:** Over 1,080 AI-related bills have been introduced across all 50 states in 2025 alone

## Universal Opt-Out Mechanisms (UOOMs)

- Required in **CA, CO, DE, MT, NE, TX, MN, NJ, NH, MD, CT, OR**
- These allow consumers to opt out of data sales/sharing via browser signals or preference settings

## Exemptions

- **B2B & Employee Data:** Exempt in most states except California
- **HIPAA, GLBA, FCRA:** Common exemptions across all laws, but scope & interpretation vary
- **Trend to limit** GLBA exemptions





forvis mazars

# Privacy Law Exemptions
# **Entities & Data Trends**

## Broad Entity Exemptions:

Many U.S. State privacy laws provide exemptions for entities subject to federal privacy laws, including HIPAA, GLBA, FCRA, FERPA, DPPA, FCA

## Trending Toward Data Exemptions:

Certain state privacy laws exempt only data subject to those laws. Organizations in California, Connecticut, Minnesota, Montana, and Oregon need to review data inventories to segregate into exempt and non-exempt data categories.

*For example, hospital employee data in California is subject to CCPA, while medical data is exempted.*

# U.S. Privacy Regulators
# **Over $3 Billion in U.S. State Law Fines in 2025**

The United States has seen a surge in litigation driven by state-level statutes and consumer empowerment, with nearly 2,500 data privacy lawsuits filed in federal courts in 2025 alone.

## Privacy Policy

$85K **Connecticut** AG settlement for privacy notice deficiencies against TicketNetwork

## Opt-Outs

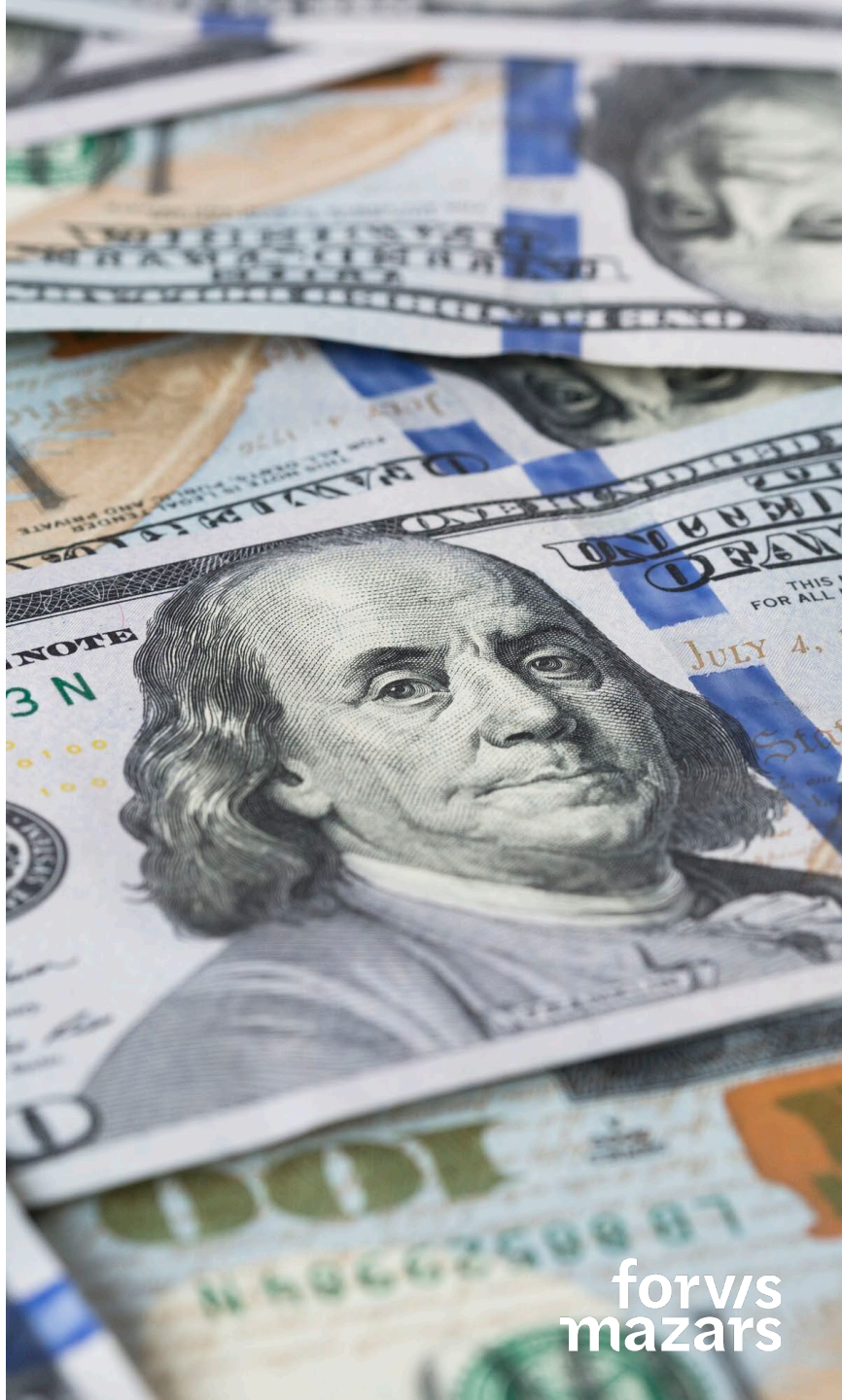
$1.55M **CCPA** settlement with Healthline Media related to defective consent management, ineffective cookie opt-outs, and purpose limitation claims

## Geolocation

Actions by **FTC, Nebraska, Indiana, Arkansas, & Texas** against GM for selling location data

## Consent

$1.4B settlement against **Google** by Texas AG for unlawful tracking and lack of consent



# Broad Enforcement
# States With & Without Privacy Laws Still Enforce Privacy Violations

## New York Privacy Enforcement Actions

NYAG resolved violations of failing to protect consumer data, resulting in $1B+ in fines issued.

**Focus on Vulnerable Populations**

The enforcement targets protect students and families by mandating stronger identity verification and security protocols.

**Managerial Compliance Importance**

Managers must ensure rigorous security measures and comply with New York's privacy laws to avoid penalties.

**Heightened Enforcement Awareness**

Organizations serving New York residents should prepare for stricter oversight on personal and sensitive data handling.

## Florida Privacy Enforcement

Florida targeted Roku for violations of children's data rights under the new Digital Bill of Rights.

## Massachusetts Data Breach Penalty

Massachusetts fined Peabody Properties $795,000 for repeated breaches and delayed incident notifications.

## Connecticut Privacy Compliance

Connecticut required TicketNetwork to correct privacy notice deficiencies and ensure ongoing compliance reporting.

# Be Aware: It’s Not Just the New State Privacy Laws

## FEDERAL TRADE COMMISSION

### FTC Privacy Enforcement

FTC focused on consumer data protection and transparency during 2025 enforcement activities. It enforces privacy using Section 5 of the FTC Act for unfair and deceptive trade practices, as well as enforcement of the GLBA.

### Avast Data Resale Case

Avast was penalized $16.5 million for reselling sensitive browsing data without user consent.

### FTC Enforcement Impact

FTC actions warn organizations to implement robust privacy policies and transparent data handling.

### Trend Toward Aggressive Oversight

Increasing FTC scrutiny signals stronger enforcement in digital advertising and consumer data use.

## Federal Communications Commission

### Combating Illegal Robocalls

The FCC focused on eliminating illegal robocalls through strict enforcement and disconnection of non-compliant providers.

### Final Removal Order 2025

In 2025, over 1,200 providers were disconnected following the FCC’s Final Removal Order to protect telecommunications networks.

### Importance of Compliance

The FCC’s actions highlight the need for organizations to comply with regulations to maintain trust and avoid penalties.

### Consumer Protection Focus

The FCC prioritizes consumer trust and security by preventing fraudulent and intrusive communications.

## U.S. Securities and Exchange Commission

### SEC Enforcement on Cybersecurity

The SEC imposed a $3.55 million penalty for inadequate data security exposing sensitive customer information.

### Privacy and Compliance Importance

Data protection is critical for compliance, investor confidence, and corporate governance in financial sectors.

### Cybersecurity Frameworks

Organizations must align cybersecurity frameworks with privacy and financial reporting standards to avoid risks.

### S-P: Privacy of Consumer Financial Information & Safeguarding Customer Information

Provides modifications to GLBA that require certain financial entities to implement privacy and security policies.





forvis mazars

# Commercial Litigation Threats

Recent years have seen a surge in privacy-related litigation, with new laws empowering consumers to take action against unauthorized data use and disclosure.

## Video Privacy Protection Act (VPPA)

VPPA prohibits nondisclosure of consumers' video viewing history without consent, protecting streaming service users.

**Consumer Rights Under the VPPA**

### Protection from Unauthorized Disclosure

Personally identifiable information (PII) cannot be shared without consent or a valid legal reason.

### Right to Consent

Consumers must give informed, written consent before PII is shared and can revoke it at any time.

### Right to Opt Out

Consumers must have a clear way to opt out of disclosure of their PII.

### Right to Notice

If PII is disclosed under a court order, consumers must be notified and allowed to contest it.

### Right to Private Action

Consumers can sue for violations, with remedies including damages, attorney fees, and other relief.

## Electronic Communications Privacy Act (TCPA)

ECPA prevents unauthorized interception of electronic communications involving tracking and wiretap technologies.

## Telephone Consumer Protection Act (TCPA)

ECPA prevents unauthorized interception of electronic communications involving tracking and wiretap technologies.

**TCPA Compliance Requirements**

- Record-Keeping
- Dialer Usage
- Caller ID
- Calling Times
- DNC List Suppression
- Required Disclosures
- Policies + Procedures
- Monitoring + Enforcement

## Fair Credit Reporting Act

FCRA ensures accuracy and privacy of consumer credit data, supporting claims after data breaches.

## Key State Privacy Laws Enabling Class Actions

### California Invasion of Privacy Act (CIPA)

Used for claims of wiretapping, eavesdropping, and digital tracking (pixels, session replay, chatbots) without consent.

### Illinois Biometric Information Privacy Act (BIPA)

Allows class actions for unauthorized collection, use, or disclosure of biometric data (fingerprints, facial scans, etc.), with statutory damages per violation.

### Washington My Health My Data Act

Expands private rights of action for health data privacy violations.

### New Jersey Daniel's Law

Protects judicial privacy and enables class actions for improper disclosure of protected information.

# Privacy Litigation vs. Roku

## One Company, One Problem, Multiple Means for Redress

**State Privacy Regulations**

States like California, Virginia, and Colorado have introduced strict privacy laws to protect consumer data and consent.

**Allegations of Data Misuse**

Roku is accused of collecting and sharing user data without proper consent, violating state privacy requirements.

**California's Leading Role**

California's strong enforcement of privacy laws sets a precedent, prompting other states to improve protections.

| Aspect | Michigan | Florida | California |
|---|---|---|---|
| **Primary Law** | COPPA + VPPA + State Privacy Acts | FDBR + Consumer Protection | CPRA + VPPA |
| **Focus** | Children’s data + video privacy | Children’s data + geolocation tracking | Children’s data + video-viewing info |
| **Penalty Model** | Federal & state statutory damages | $150K per violation under FDBR | CPRA statutory penalties + class action damages |
| **Unique Risk** | Multi-layer enforcement (federal + state) | First FDBR case; “willful disregard” | Dual track: regulatory + private litigation |

# Children’s Privacy
# COPPA 2.0 & Age Assurance

### State-Specific Age Verification

Texas, Utah, and Louisiana require commercially reasonable methods to verify user age with four age categories.

### California's Age Gate Requirement

California mandates an age input interface during account setup categorizing users under 18 as children.

### Purpose of Verification Laws

The laws aim to appropriately identify and protect minors in digital environments through age categorization.

### State-Based Verification Responsibility

Texas, Utah, and Louisiana assign age verification to the account creator, either minor or parent. California requires explicit parental verification.

### Parental Involvement Emphasis

California law increases parental responsibility, impacting how minors access digital services compared to other states.

### Impact on Developers & Platforms

App developers must tailor age verification processes to comply with varying state laws, affecting user flow design.

# Chatbots
# Privacy Regulatory Concerns

### Transparency & Disclosure

Users must be clearly informed when interacting with an AI chatbot, especially minors. Ongoing and prominent notices are required.

### Consent & Data Collection

Chatbots often collect sensitive personal data. Regulations demand explicit, informed consent—especially for sensitive categories and children. Standard privacy notices may not be sufficient for U.S. state laws.

### Automated Decision Making & Profiling

Use of automated decision making or profiling triggers additional requirements. Organizations must disclose decision logic, provide opt-out mechanisms, and ensure fairness.

### Data Minimization & Retention

Data collection must be limited to what is strictly necessary, with strict retention and deletion requirements. Chatbots should avoid unnecessary data capture.

### Security & Safeguards

Robust security measures are required to protect user data from unauthorized access and breaches. Regular risk assessments, breach response plans, and vendor audits are expected.

# Artificial Intelligence
# **High-Risk AI Use Cases**

## EU AI Act

| Section & Category | Use case |
|---|---|
| **Biometrics** | Remote biometric identification, biometric categorization, emotion recognition |
| **Critical Infrastructure** | Safety components in digital infrastructure, traffic, utilities |
| **Education & Training** | Admissions, evaluations, behavior monitoring |
| **Employment** | Recruitment, promotion, termination, task allocation, performance monitoring |
| **Essential Services** | Access to healthcare, social security, housing, credit scoring |
| **Law Enforcement** | Risk assessments, evidence analysis, crime prediction |
| **Migration & Borders** | Identity verification, eligibility assessments |
| **Justice & Democracy** | Judicial decision making, democratic participation |

## Examples of U.S. State Laws

**California:** Multiple bills, including the AI Transparency Act (SB 942) and Frontier AI Transparency Act (SB 53), effective in 2026

**Colorado:** Colorado AI Act (SB 205), effective February 2026

**Texas:** Texas Responsible AI Governance Act (TRAIGA), effective January 2026

**Utah:** UAIPA (SB 149), effective May 2024

## Key Takeaways

- No unified federal law
- Patchwork of state laws
- ~186 state AI laws enacted as of 12/25
- Over 1,000 bills introduced in recent sessions
- Laws cover transparency, bias, data privacy, & accountability



forvis mazars

# Upcoming Cyber Reporting Requirements


Companies that process more than 250,000 consumers' personal information and to which the CCPA applies will need to conduct cybersecurity audits.

Phased implementation timeline based on 2026 gross revenue:

- More than $100 million by April 1, 2028
- $50 million to $100 million by April 1, 2029
- Under $50 million by April 1, 2030

After initial audit, annual audits, for the prior year must be completed by April of the current year.

A cybersecurity audit is far more than a compliance checkbox—it's a strategic tool that strengthens defenses, streamlines operations, and builds stakeholder confidence. When integrated into a comprehensive compliance framework, it helps organizations proactively mitigate risks, avoid regulatory penalties, and prevent reputational and operational fallout.



forvis mazars

# 02

PCI

# What Is PCI DSS?

**Payment Card Industry Data Security Standard**

- PCI DSS is a global data security standard for protecting payment data:
- Credit and debit card transactions

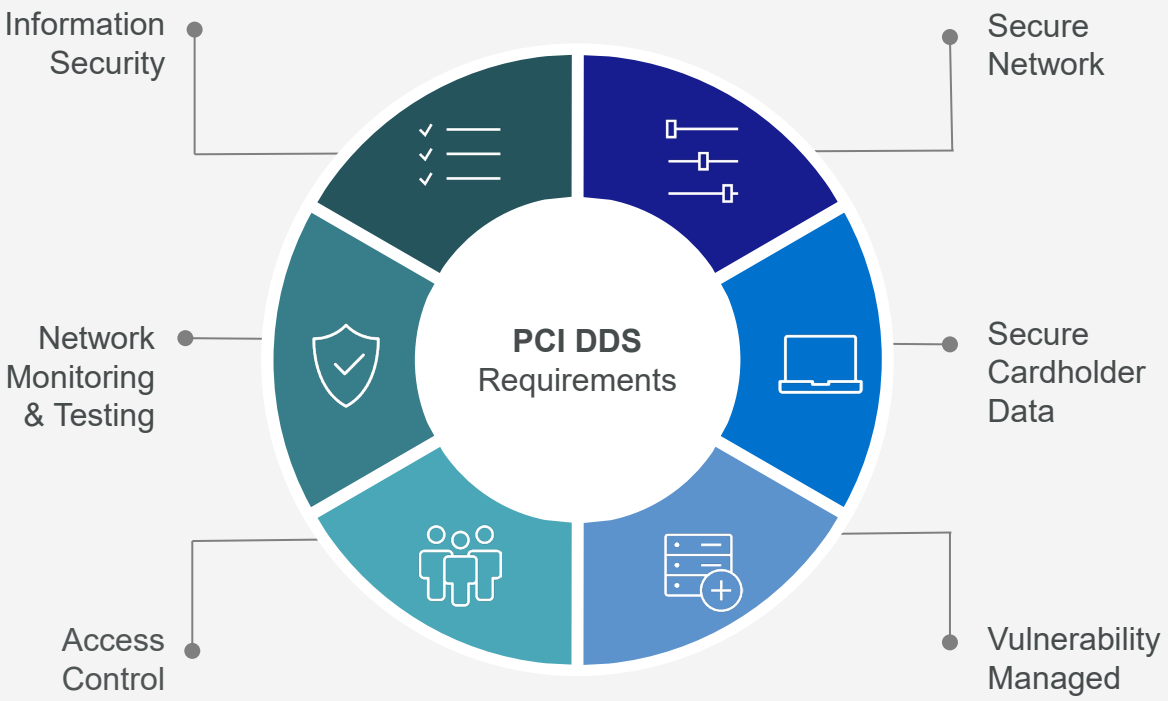
**Mature standard, has been in existence since 2005**

- Superseded individual card brand standards going back to 2001
- Developed to encourage and enhance payment card account data security and facilitate the broad adoption of consistent data security measures globally

**Provides a baseline of technical and operational requirements designed to protect account data**

- Extensive, technical security standard covering range of security controls – system and application security, cryptography, process and operations, policies and governance

**Most recent version is 4.0.1**

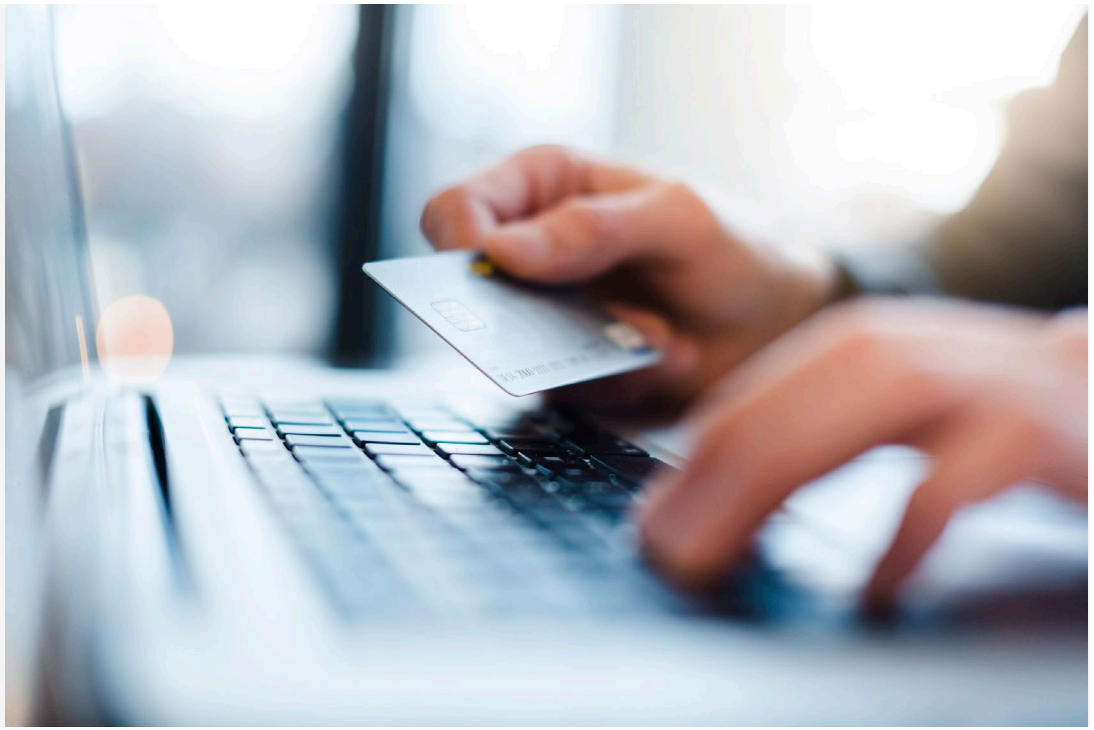


# What Is Cardholder Data?

| | | Data Elements | Storage Restrictions | Required to Render Stored Data Unreadable |
|---|---|---|---|---|
| Account Data | Cardholder Data | Primary Account Number (PAN) | Storage is kept to a minimum as defined in Requirement 3.2 | Yes, as defined in Requirement 3.5 |
| | | Cardholder Name | Storage is kept to a minimum as defined in Requirement 3.2 | No |
| | | Service Code | | |
| | | Expiration Date | | |
| | Sensitive Authentication Data | Full Track Data | Cannot be stored after authorization as defined in Requirement 3.3.1 | Yes, data stored until authorization is complete must be protected with strong cryptography as defined in Requirement 3.3.2 |
| | | Card verification code | | |
| | | PIN/PIN Block | | |

# Who Is the PCI DSS Intended For?

- All entities that store, process, or transmit cardholder data (CHD) and/or sensitive authentication data (SAD)
- Or could impact the security of the cardholder data environment (CDE)
- All entities involved in payment account processing – merchants, processors, acquirers, issuers, and other service providers



# Who Is the PCI DSS Intended For?

## The Payment Brands are responsible for defining the levels for Merchants and Service Providers for the data security programs.

The level of a Merchant or Service provider is based on the transaction volume of credit card transactions. Transaction volume is determined by card brand, not as a whole. An Acquirer may consolidate all transaction volume for multiple brands.

### Visa Merchant Levels and Reporting Requirements

| Level | Criteria | Requirements |
|---|---|---|
| **Level 1** | Merchants processing over 6 million Visa transactions annually across all channels or Global merchants identified as Level 1 by any Visa region | Every year:<br>• File a Report on Compliance ("ROC") by Qualified Security Assessor ("QSA") or internal resource if signed by officer of the company<br>• Submit an Attestation of Compliance ("AOC") Form |
| **Level 2** | 1 to 6 million Visa transactions annually across all channels | Every year:<br>Complete and submit Self-Assessment Questionnaire ("SAQ") |
| **Level 3** | Less than 1 million Visa ecommerce transactions annually across all channels | Every year:<br>Complete and submit Self-Assessment Questionnaire ("SAQ") |

### Visa Service Provider Levels and Reporting Requirements

| Level | Criteria | Requirements |
|---|---|---|
| **Level 1** | Merchants processing over 6 million Visa transactions annually across all channels or Global merchants identified as Level 1 by any Visa region | Every year:<br>• File a Report on Compliance ("ROC") by Qualified Security Assessor ("QSA") or internal resource if signed by officer of the company<br>• Submit an Attestation of Compliance ("AOC") Form |
| **Level 2** | 1 to 6 million Visa transactions annually across all channels | Every year:<br>Complete and submit Self-Assessment Questionnaire ("SAQ") |

# Dispelling Some Myths

### “I don’t store credit card data”

Can still have obligations for transmission or connectivity

### “My third-party handles all of this”

At the very least, some oversight responsibility

### “I have a certificate of compliance”

Assessment or validation, not certification

### “We aren’t a Level 1, so we don’t need it”

Levels are about transaction volume and determined by payment brands; sometimes this determines what reporting is used

# Questions to Ask

- Do you accept payments for your services through credit/debit cards?
- Have clients asked about cardholder processes and systems' security and are they requesting a PCI attestation of compliance (AOC) be provided?
- Does your organization provide business services for other companies that conduct transactions with credit/debit card data?
- In your daily business processes, do you have access to or hold within your systems credit/debit card data?
- What specific data security or privacy regulations does your organization need to comply?
- Do you have a contract with a processor or acquiring bank to process your card transactions?

# 03

## HIPAA

# Importance of Privacy Across Sectors

### Critical Role of Privacy

Privacy builds trust and ensures compliance across healthcare and other industries by protecting sensitive personal data.

### Risks of Non-Compliance

Failure to protect sensitive data leads to financial penalties, reputational damage, and loss of consumer trust.

### Privacy Regulations Overview

Regulations like HIPAA, GDPR, and CCPA set standards for protecting personal data in healthcare and beyond.

### Implementing Privacy Measures

Organizations should adopt best practices and enforce policies to safeguard sensitive information effectively.

# Healthcare Regulations
# HIPAA

### HIPAA Overview & Rules

HIPAA sets national standards to protect health information via Privacy and Security Rules.

### Enforcement & Penalties

The OCR enforces HIPAA, issuing millions in penalties for violations since 2003.

### Common Violations

Frequent violations include unauthorized disclosures, inadequate safeguards, and access failures.

### Risk Mitigation Strategies

Risk assessments, multi-factor authentication, and breach notifications are vital compliance steps.

# HIPAA Enforcement

Office for Civil Rights

**OCR Enforcement Actions - HIPAA**

OCR resolved 12 settlements in 2025 addressing privacy and security HIPAA violations.

**Common Compliance Issues**

Issues include inadequate risk analysis, insufficient breach notifications, and lack of staff training.

**Proactive Compliance Strategies**

Prioritize audits, employee training, and incident response to mitigate privacy risks effectively.

**Regulatory Trends**

Regulators focus on proactive compliance rather than reactive responses to enhance resilience.

# Non-Healthcare Regulations
# GDPR & CCPA

### Overview of GDPR

GDPR governs data processing for EU citizens, enforcing strict consent, transparency, and security requirements to protect personal data.

### GDPR Enforcement & Fines

Fines under GDPR can reach 4% of global turnover, with major penalties like Meta's €1.2 billion fine for data violations.

### CCPA Consumer Protections

CCPA focuses on California consumer rights and transparency, promoting data privacy and control over personal information.

### Compliance Best Practices

Robust compliance requires consent management, data minimization, and vendor oversight to meet GDPR and CCPA standards.

# Navigating Complexity

- The shift from voluntary compliance to active enforcement
- The need for proactive risk management and privacy impact assessments
- Privacy audits and vendor risk management assist in enforcement readiness
- Prioritize transparency and control
- Update and monitor
- Understand the Regulatory Landscape

# Thank You

Questions?

# Contact

## Forvis Mazars

**Nikole Davenport**
Director, Privacy – IT Risk & Compliance
404.272.8439
nikole.davenport@us.forvismazars.com

**Diana Ramirez**
Manager, Healthcare Privacy – IT Risk & Compliance
213.282.8713
diana.ramirez@us.forvismazars.com

**Darin McLaury**
Director – IT Risk & Compliance
972.897.7069
darin.mclaury@us.forvismazars.com

The information set forth in this presentation contains the analysis and conclusions of the author(s) based upon his/her/their research and analysis of industry information and legal authorities. Such analysis and conclusions should not be deemed opinions or conclusions by Forvis Mazars or the author(s) as to any individual situation as situations are fact-specific. The reader should perform their own analysis and form their own conclusions regarding any specific situation. Further, the author(s)' conclusions may be revised without notice with or without changes in industry information and legal authorities.