

The Next Wave: Navigating Privacy Requirements



Your speakers



Laurel Sykes, CRCM
EVP, Chief Risk Officer
American Riviera Bank



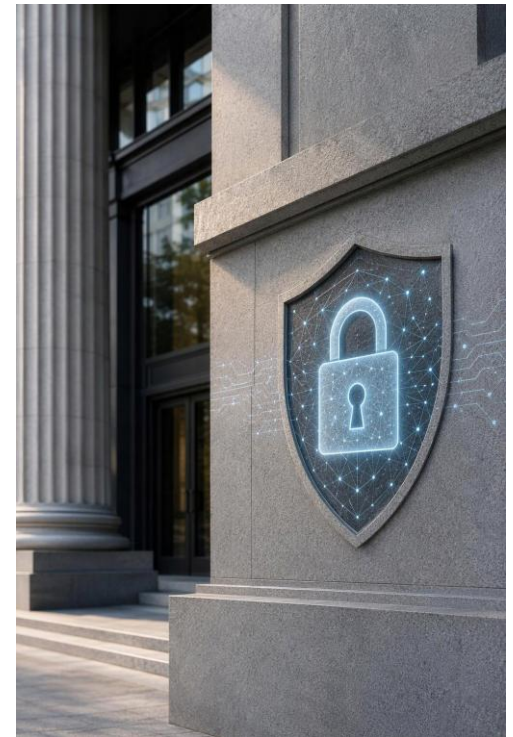
Paul Abramson
EVP, Chief Technology Officer
American Riviera Bank



Doug DePeppe
Special Counsel, Buchalter LLP
Co-Chair, Cyber Investigations

Agenda

- Scope: banks, GLBA and CCPA
- CCPA Mission and the Data Broker Problem
- State of Enforcement and Litigation Risk
- Privacy Risk Assessments
- Disclosure Obligations
- Cybersecurity Audit Coverage
- Building your compliance program



What's new for 2026 and 2027

Risk assessments

- Required for processing “sensitive personal information” (e.g. sensitive PI, large-scale profiling, location tracking) or using ADMT to make “significant decisions” by April 1, 2028

Automated decision-making

- Disclosure, opt-out, notice, opt-out, and limitation on use duties begin January 1, 2027

Cybersecurity audits

- Annual audits, first certifications due April 1, 2028 – April 2030 based on size (revenue)

Enforcement / Private Right of Action

- A strike force now targets data broker registration failures
- Increasing cases and demand letters related to California Invasion of Privacy Act

1. DROP deletion requests start August 1, 2026
2. SB 361 broker disclosures began January 1, 2026
3. Built-in browser opt-out signals by January 2027
4. Revenue threshold now \$26.625M

Threshold Question: What Bank Data Is in Scope?

Start with the data and processing activity, not the institution's label.

Potentially exempt under GLBA

- Personal information collected, processed, sold, or disclosed pursuant to GLBA and implementing regulations
- Exemption is data-level, not an automatic institution-wide exclusion

Often remains in CCPA scope

- Employees and job applicants
- Prospects and noncustomer visitors
- Website identifiers, cookies and ad-tech data
- Certain affiliate, marketing, and commercial data
- Activities outside the GLBA purpose and relationship

Practical rule: classify each data flow, purpose, recipient role, and statutory exemption.

PART 1

CPPA Mission & the Data Broker Problem

Why CCPA Enforcement Is Structural, Not Reactive

Maximum ordinary violation

\$2,663

Intentional / known under-16

\$7,988

Audits

**Announced or
unannounced**

- California's Constitution expressly protects privacy.
- The CCPA has rulemaking, audit, investigation, administrative enforcement, and penalty authority.
- There is no mandatory statutory cure period before enforcement.
- Failure to cooperate with an audit can lead to compulsory process.

Operational compliance matters: working rights processes, accurate notices, configured technology, and enforceable vendor controls.

The Data Broker Problem and Why Banks Should Care

Registered brokers

580+

Active in DROP

600+

Deletion requests

345K+

Identifiers

1.3M+

DROP milestones

- January 2026: platform and regulations effective
- August 1, 2026: processing begins
- Brokers access and process requests at least every 45 days

Banking issue spot

- Some marketing, enrichment, identity, analytics, or fraud vendors may separately operate as data brokers.
- Determine whether each vendor acts only as a service provider or also uses data for independent commercial purposes.

PART 2

Enforcement: End of 2026 and Into 2027

Enforcement Posture: What Regulators Can See

GPC / OOPS

Signal received but sale or sharing continues

Broken opt-outs

Link, toggle, or preference center fails

Rights friction

Excessive verification, asymmetry, or extra steps

Notice mismatch

Disclosure does not match actual trackers or uses

Vendor gaps

Contracts and operational controls do not align

For authenticated users, an opt-out preference signal may need to be applied beyond the current browser or device.

Recent Enforcement: The Pattern That Emerges

Matter	Year	Penalty	Primary lesson
General Motors	2026	\$12.75M	Driving/location data; purpose limitation and minimization
Disney	2026	\$2.75M	Opt-out failed across associated services and devices
Tractor Supply	2025	\$1.35M	Notices, applicants, GPC, contracts
Honda	2025	\$632.5K	Verification, asymmetry, authorized agents, contracts
Todd Snyder	2025	\$345.2K	Misconfigured portal; excessive verification

Pattern: friction, broken implementation, notice gaps, and vendor controls are independently actionable.

PART 3

Legal Risk: CIPA and CCPA Class Actions

CIPA: A Separate, Unsettled Private-Litigation Track

CIPA is not the CCPA

- Distinct statutory elements, defenses, standing questions, and remedies
- Rapidly evolving theories involving website technologies
- Avoid treating demand-letter allegations as settled law

Common issue-spotting targets

- Advertising pixels and SDKs
- Session-replay tools
- Third-party chat and support tools
- IP lookup and attribution services

Risk-control approach

Inventory technologies, document data flows and recipient roles, align notices and contracts, and assess whether particular tools should be blocked before consent based on CIPA and other applicable regimes.

CCPA Data Breach: Statutory Exposure Calculator

Private right of action

- \$107–\$799 per consumer per incident, or actual damages if greater
- Applies to specified nonencrypted and nonredacted information
- Requires a security incident resulting from failure to maintain reasonable security

Encryption and related controls

- Analyze the actual statutory data set and the control in use
- Encryption, tokenization, hashing, and key management are not interchangeable
- Avoid categorical “safe harbor” statements without a fact-specific review

Consumers	\$107 floor	\$799 ceiling
10,000	\$1.07M	\$7.99M
50,000	\$5.35M	\$39.95M
100,000	\$10.70M	\$79.90M
250,000	\$26.75M	\$199.75M
500,000	\$53.50M	\$399.50M
1,000,000	\$107.00M	\$799.00M

Gross theoretical range before standing, class certification, defenses, causation, and settlement considerations.

Privacy Risk Assessment

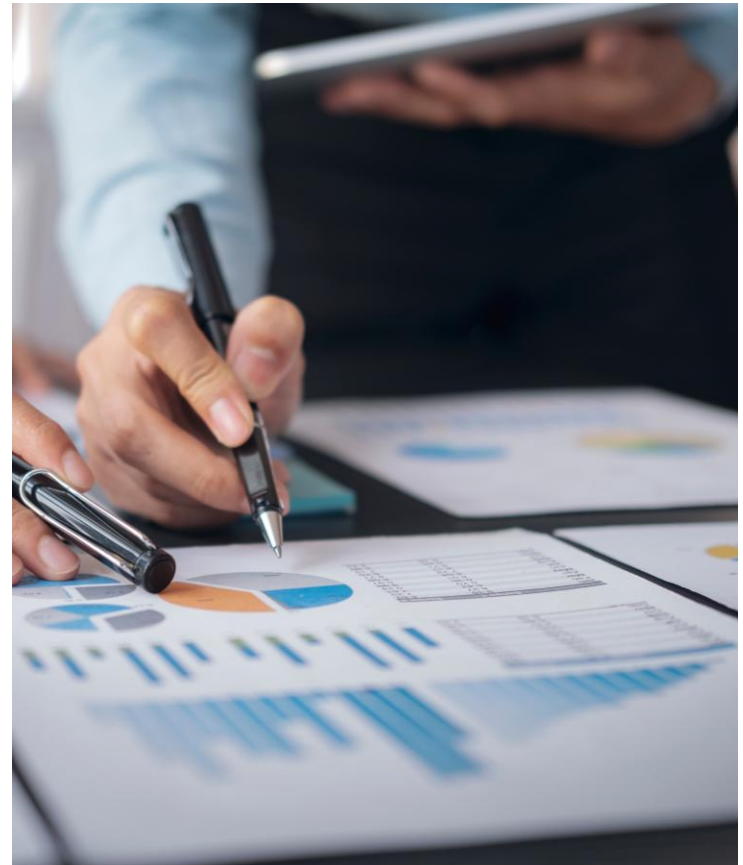
You must determine whether the risks to consumers' privacy outweigh the benefits to the consumer, the business, other stakeholders, and the public from that same processing

Mapping Data Flows: Where may your obligations be hiding?

- Websites that track sensitive data.
- Consumer data related to business transactions, such as loan applications or signers on deposit accounts
- Employee data, or data on consumers who have applied for jobs with your bank

Remember

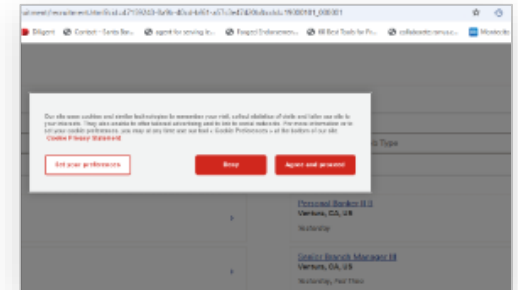
Consumers have the right to limit the use of their "sensitive personal information"—such as IP address and geolocation—to specific purposes.



Website: “Do not sell or share.”

- **Eliminating “Do not Sell” Triggers on Website**

- Track activity by session, not cookie
- Anonymize specific information
- Favor general over specific (e.g. City/State instead of GPS coordinates)
- Capture campaign, lead-gen, social and referrer data without tying it to an individual
- Opt-in via form submissions or “call to action” links



- **Your vendors may still track activity**

Example: What tracking can look like without identifying the individual

1. Identifiers deliberately left out

- a. Full or partial IP address stored against a visit
- b. Persistent cookie or device ID linking sessions over time
- c. Precise geolocation or household-level address
- d. Cross-site profiles built with third-party ad tags
- e. Names or emails, except where the visitor opts in through a form



Session-level behavior: 12,480 sessions, avg 2:14 on page, 38% reached loan page



Aggregated geography: 62% from California, led by Sacramento and Fresno — city/state only



Traffic source and campaign: 41% organic, 22% paid social, 15% email — no visitor identity



Device and browser class: 68% mobile, 30% desktop — no fingerprint or persistent ID



Event and conversion counts: 310 calculator uses, 94 appointments, 27 applications — totals only

19

- 2. Identity enters the record only when the visitor chooses to give it.

Less data may not help: California Invasion of Privacy Act

Website trackers are under fire

Some capture very little; others follow users across the internet

Less data may not help as claims have been filed over limited anonymous data



Third-party cookies

Stored on the user's browser and owned by a third party with direct access



Third-party pixels

Embedded code that reports site activity to the operator and the pixel owner at once



Device fingerprinting

A third party matches anonymous data to its own database to reveal identity



Analytics software and tools

Send user data out for automated analysis

Poll question: Do you know if your marketing team is making inferences on click choices or purchase decisions to retarget on your website?

Privacy Risk Assessment: the details matter

Consider the data elements to provide:

- Method of interaction
- Method of collection and use
- Categories collected
- Purpose of each use
- Retention periods
- Number of consumers
- What disclosures have been made and how
- Third parties
- Any use of ADMT

SAMPLE PRA REPORT CERTIFICATION

Business and contact Northwind Retail, Inc. Dana Ruiz, Privacy Officer, (415) 555-0142

Period covered January 2026 through December 2026

Assessments 14 total: 6 selling or sharing, 4 sensitive PI, 3 ADMT decisions, 1 ADMT training

Categories Identifiers, commercial, internet activity, geolocation. Sensitive: precise geolocation, log-in credentials

Attestation *"Under penalty of perjury... the risk assessment information submitted is true and correct."*

Signed Dana Ruiz, Chief Privacy Officer, April 1, 2027

Sample Assessment Form

PRA Assessment Form (copy this sheet per activity if desired)							
PRA ID	CL-01						
Business Line	Commercial Lending						
Processing Activity	Underwriting						
Owner							
Reviewer							
Approver							
Trigger(s)							
Purpose (specific, non-generic)	Approve guarantors						
Systems / Technology	Sageworks						
Third Parties / Vendors	Abrigo						
Approx. # Consumers Impacted							
Disclosures (where/how)							
Retention (by category)							
Decision							
Status							
Data Inventory & PI Category Matrix (Required)							
Data Element / Field	PI Category (CCPA)	SPI? (Y/N)	Source	Purpose of Use	Shared With	Retention Period	Data Classification
Social Security Number	Identifiers	Y	Personal Financial Statement	Underwriting	Abrigo		
Name	Identifiers	N	Personal Financial Statement	Identify guarantor	Abrigo		
Email	Personal Records	N	Personal Financial Statement	Contact guarantor	Abrigo		
Login	Geolocation Data	Y	Sageworks	Collect Esignatures	Abrigo		
Company name	Commercial Information	N	Tax returns	Underwriting	Abrigo		
Position	Professional/Employment Information	N	Personal Financial Statement	Underwriting	Abrigo		
Income information	Professional/Employment Information	N	Tax returns	Underwriting	Abrigo		
FICO		N	Credit report	Underwriting	Abrigo		

Control Library

Control ID	Control Name	Control Type	Owner Role	Mapped CCPA PRA Element	Mapped GLBA/FFIEC/NIST	GLBA / NIST Control ID	Evidence Examples	Applicable PI Categories
GOV-01	PRA governance, roles, and approval workflow	Administrative	CRO/Compliance	Proceed decision + approvals + contributors	FFIEC Governance; GLBA oversight	ID.RA-04 / ID.IM-01	RACI; approvals; committee minutes	All
INV-01	PI/SPI inventory maintained and refreshed	Administrative	Privacy/Compliance	Categories of PI/SPI and minimization	FFIEC Identify		Data map; data dictionary	All
NOT-01	Consumer disclosures and just-in-time notices	Administrative	Compliance/Marketing	Consumer relationship & disclosures	GLBA Privacy Rule		Notice versions; change logs	Identifiers;Commercial Information;Internet/Electronic Activity
CRR-01	Consumer rights request process (access/deletion/opt-out)	Administrative	Compliance/Operations	Safeguards and mitigations	Operational controls		SOPs; tickets; QA	All
VND-01	Vendor contracts require safeguards + breach notification	Vendor	Vendor Mgmt	Third parties / recipients	GLBA service provider oversight	GV.SC-02 - GV.SC-06	Contracts; SOC reports; DD	All
ACC-01	Least privilege access + recertification	Technical	IT/InfoSec	Safeguards and mitigations	NIST PR.AA; FFIEC Access	PR.AA-01 / PR.AA-02 / PR.AA-05	Access reviews; IAM logs	All
ENC-01	Encryption at rest and in transit	Technical	IT/InfoSec	Safeguards and mitigations	NIST PS.DS	PS.DS-01 / PR.DS-02	Configs; key mgmt	Identifiers;Commercial Information;Geolocation Data;Biometric Information
DLP-01	DLP monitoring for email/web/file sharing	Technical	IT/InfoSec	Safeguards and mitigations	NIST DE.CM	DE.CM-09	Alerts; incident records	Identifiers;Commercial Information;Internet/Electronic Activity
IR-01	Incident response & breach notification	Administrative	IT/InfoSec	Safeguards and mitigations	FFIEC Respond/Recover	PR.IR-01	IR plan; tabletops	All
TRN-01	Privacy & security training	Administrative	HR/Compliance	Safeguards and mitigations	NIST PR.AT	PR.AT-01 / PR.AT-02	Training completion	All
ADMT-01	ADMT/model governance (bias checks, oversight, appeals)	Administrative	MRM/Compliance	Technology used (incl. ADMT logic/outputs if applicable)	Model risk mgmt	ID.RA-06	Model docs; bias testing	Inferences/Profiling Outputs;Protected Characteristics;Commercial Information

Disclosure Obligations for Privacy Notice and Pre-Use and Opt-Out for ADMT

Thinking through the Implications of ADMT

Disclosable inferences creating a profile about a consumer

- Offering products using marketing technology or data based on purchasing or browsing decisions?
- Identity inferences that might lead you to derive information, data, assumptions, or conclusions regarding identity of a potential signer to approve an account?
- Automated small business loan dec

Is opt-out required?

- You do not need to provide for ADMT opt-out if you provide consumers with a method to appeal the decision

What the pre-use notice must cover

- Plain-language purpose of the ADMT
- How to opt out—or how to appeal, if using that exception
- Right to access ADMT information; no retaliation for using rights
- Additional information about how the ADMT works and how the output is used in the decision
- Opt-out: at least two methods, one matching how you usually interact

Poll question: Does your bank leverage any ADMT that might trigger the notice and opt-out requirements?

Do disclosures match actual collection?

- Does every tracker and form field map to a disclosed category and purpose?
- Are categories of third-party recipients and retention periods stated accurately?
- Do opt-out signals actually stop tags from firing?

15	Biometric information: includes fingerprints and voiceprints;
16	Internet or network activity information: browsing history and interactions with our website;
17	Geolocation data: <u>includes</u> device location and Internet Protocol (IP) address;
18	Audio, electronic, visual and similar information: call and video recordings;
19	Professional or employment-related <u>information</u> : includes work history and prior employer as part of your employment with American Riviera Bank;
	Education information: may include student records or directory information; and
20	Inferences drawn from any of the Personal Information listed above: used to create a profile or biography about, for example, an individual's background and qualifications, social media URL, etc.

1

Inventory what you say

Privacy policy, notice at collection, cookie banner

2

Scan what you collect

Tags, pixels, cookies, SDKs, and form fields on every site and app

3

Map and compare

Match each data element to a disclosed category, purpose, and recipient

4

Close the gaps

Remove the tracker or update the disclosure, then re-test on a schedule

Poll question: Has your bank compared its privacy disclosures to what you actually collect?

Cybersecurity Audit Requirements

Who must audit?

- 50%+ of annual revenue from selling or sharing personal information, or
- Revenue above the CCPA threshold (\$26.625M) and, in the prior year, processed:
 - **250,000+** consumers' personal information, or
 - **50,000+** consumers' sensitive personal information

What is required?

- Annual independent audit (internal or external)
- Covers MFA, encryption, access controls, vulnerability testing, incident response
- Executive-signed certification to the CPPA
- Due April 1: 2028 (>\$100M revenue), 2029 (\$50–100M), 2030 (<\$50M)

Poll question: Has your bank determined that its non-GLBA data triggers an audit?

Three Actions Before Year-End 2026

01

Scope, Notice, Tracker & GPC Audit

- Map GLBA-exempt and nonexempt data flows
- Test GPC/OOPS while logged out and logged in
- Confirm notices match trackers and recipients
- Validate opt-out status and downstream suppression

02

Vendor Role & Contract Review

- Classify service provider, contractor, third party, or data broker
- Include required §§ 7050–7051 restrictions
- Test actual use, onward transfers, and cooperation rights
- Remediate contracts and configuration together

03

Security & Incident Readiness

- Map statutory breach data and protection state
- Evaluate encryption, tokenization, hashing, and keys
- Document reasonable-security controls
- Add day-one breach scoping to the response plan