FRONT-BURNER REGULATORY ISSUES

AGENDA

- Session Overview
- Understanding the dynamic compliance landscape for 2026
- Translating regulations into practical strategies
- Next Steps

REGULATORY LANDSCAPE

- Evolving privacy laws and implications, including use of ADMT
- Shifting fraud liability and California legislature
- Fair banking / debanking Risks
- Pending status of Section 1071 rule
- Updates in BSA (Bank Secrecy Act) and cybersecurity risk assessments
- Third party risk management best practices

EVOLVING PRIVACY ISSUES

CALIFORNIA CONSUMER PRIVACY ACT,
CHILDREN'S ONLINE PRIVACY ACT

CALIFORNIA CONSUMER PROTECTION ACT (CCPA) CALIFORNIA PRIVACY RIGHTS ACT (CPRA)

- CCPA/CPRA may apply to employee data, vendor data, website data, and marketing data.
- Banks must segregate GLBA data (exempt) vs. non-GLBA data (covered).
- Banks must disclose the **categories** of personal information they collect, the **business purposes** for collecting it, and the categories of third parties with whom they share it. A prominent link titled "Do Not Sell or Share My Personal Information" must be visible on their website.
- Consumers have the right to limit the use of their "sensitive personal information"—such as Social Security numbers and geolocation—to specific purposes.
- **Consumer rights requests**: Banks must have procedures in place to honor consumer requests, including:
  - **Right to know**: The consumer's right to request access to the personal information a bank has collected about them.
  - **Right to delete**: The consumer's right to request the deletion of their personal information.
  - **Right to correct**: The right to request the correction of inaccurate personal information.
- Banks must implement and maintain **reasonable security measures** to protect against data breaches involving unencrypted or unredacted personal information. Failure to do so can expose the bank to private lawsuits
- Banks that process a significant amount of personal information or exceed certain revenue thresholds may be required to conduct and submit comprehensive, regular **cybersecurity audits**.
- Vendor contracts must include specific provisions restricting how the third party can use personal information.

CALIFORNIA PRIVACY PROTECTION AGENCY (CPPA) REGULATIONS

Recent updates effective January 1, 2026

- Mandatory **independent cybersecurity audits** for businesses posing "significant risk" (based on revenue, data sensitivity, processing scale). Staggered compliance: 2028–2030 deadlines for filing certifications with CPPA.
- Formal **Privacy impact risk assessment requirement** for high-risk processing (e.g. sensitive PI, large-scale profiling, location tracking). Must maintain records + submit attestations to CPPA by 2028.
- New **Automated Decision-Making Technology (ADMT) rules** (covering automated systems making significant consumer decisions). Disclosure, opt-out, and limitations on use. Goes live **Jan 1, 2027**. Explicit term "AI" was dropped; rules use tech-neutral definition of ADMT.
- **Opt-in / Opt-out Timing** Businesses must wait **12 months before re-asking** a consumer who opted out of sale/sharing to opt back in.

Proposed Accessible Deletion Mechanism Regulations
(Public comment period closed August 18, 2025)

- The "Delete Act" (SB 362) requires the CPPA to set up an *accessible deletion mechanism* through which California consumers can submit a single deletion request to all registered data brokers. The DROP (Delete Request and Opt-out Platform) is intended to be that mechanism.
- Under the proposals, the DROP must be functional for consumers by January 1, 2026; data brokers must begin using it by August 1, 2026.

PRACTICAL CONSIDERATIONS

Where Might ADMT Come into Play?

- Must notify consumers of ADMT use in Significant Decisions who fall outside of the GLBA exemption
  - Do you use automated decisioning technology in your business lending function to "substantially replace" human decision making?
  - Does your HRIS system "score" or otherwise decision job applicants as part of the initial screening process?
  - Do you use ADMT in hiring to profile in a way that would disqualify someone for a job?
  - What sort of technology is used to determine offers of financial services for prospective clients?

Cybersecurity Audit Considerations

- Cybersecurity audit threshold is triggered if you are over the $25 million revenue threshold, and processing
  - The personal information of over 250,000 California consumers or households, or
  - The sensitive personal information of over 50,000 California consumers or households - how will you determine everywhere you process sensitive consumer data, such as geolocation?
- Are you able to leverage cybersecurity reports prepared for another purpose and do they comply with all regulatory requirements?

PRACTICAL IMPLICATIONS

Privacy Risk Assessment Considerations

- Privacy risk assessments are required when processing personal information presents "significant privacy risks" or using ADMT to make "significant decisions"
  - Notices are fairly boilerplate as to what data is covered, but have you reviewed each of your business lines to determine data points such as
    - Methods for collecting the data
    - The benefits of collecting
    - The number of consumers impacted
  - How will you determine "potential negative impacts" and ensure against non-discrimination?
  - Who will be named in the assessment?

Are you considering all disclosable data?

- Disclosable inferences creating a profile about a consumer to predict, target or affect consumer behavior
  - Marketing technology or data based on purchasing or browsing decisions?
  - BSA inferences that might lead you to derive information, data, assumptions, or conclusions regarding identity of a potential signer?
- Are you responding to consumer requests?
  - How do you respond to requests about "inferences" under RTK?
  - Is precise geolocation data collected on your website for visitors to your site? If so, do consumers have a RTD?

CHILDREN'S ONLINE PRIVACY PROTECTION ACT (COPPA) CALIFORNIA AGE-APPROPRIATE DESIGN CODE ACT

- **COPPA (Children's Online Privacy Protection Act, Federal)**
  - Applies to the online collection of personal information from children under age 13.
  - Requires a clear privacy policy, parental notice, and "verifiable parental consent" before collecting, using, or disclosing personal info from children under 13.
  - Limits use of the collected information, mandates data security, prohibits requiring more information than necessary, and requires deletion when no longer needed.
- **California's AB 2273 (Age-Appropriate Design Code Act)**
  - Applies to online services **likely to be accessed by children under age 18.**
  - Prohibits using a child's personal information by default, collecting or retaining geolocation data, profiling children by default, and leading or encouraging children to provide personal data.
  - Requires a **Data Protection Impact Assessment** (DPIA) for new online services, products, or features likely to be accessed by children.
  - Currently subject to a **partial injunction** on data collection, requiring design changes, and data assessments pending litigation.

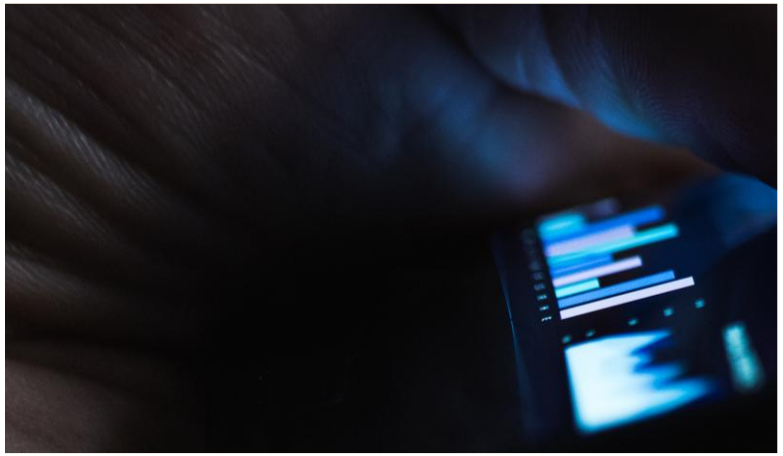
CHILDREN'S ONLINE PRIVACY RECENT CHANGES

COPPA Changes (effective June 23, 2025)

- **Broader definition of "personal information":** Expanded to include biometric identifiers like fingerprints and facial patterns.
- **Enhanced parental consent:** Requires separate, verifiable parental consent for disclosing a child's information to a third party, unless the disclosure is "integral" to the service.
- **Data retention limits:** Prohibits the indefinite retention of a child's personal information and requires operators to establish a written data retention policy.
- **Written security program:** Mandates that operators implement a written security program to protect children's personal information.
- **"Mixed audience" services:** Provides clarification for websites that have both child and adult users, requiring age screening before collecting any personal data.

California's Protecting Our Kids from Social Media Addiction Act (SB 976)

- This law, signed in September 2024 and initially set to take effect on January 1, 2025, the act prohibits platforms from providing an "addictive feed" to minors without verifiable parental consent and bans notifications during school hours and late at night.
- Challenged on free speech grounds, the 9th Circuit recently upheld the "addictive feed" restrictions but ruled that banning metrics like "likes" was unconstitutional.
- **Ongoing legal challenge:** A lawsuit filed by the tech trade group NetChoice has challenged the law's constitutionality, alleging it violates free speech. The case has been sent back to the district court for further proceedings.



SHIFTING FRAUD LIABILITY

Regulation E – 2021 FAQs from the CFPB

Federal scrutiny regarding Regulation E liability

NACHA's Operating Rules include Fraud Monitoring Amendments

California legislature

REGULATION E FAQS DECEMBER 2021

Bank Impersonation Scams Covered

Regulation E FAQs clarify that bank impersonation scams causing 'unauthorized' transactions are protected under EFTA guidelines.

Consumer Losses Eligible for Reimbursement

Consumers affected by such scams may qualify for reimbursement if they were defrauded into providing credentials and did not perform the transfers.

Banks Must Review Claims Carefully

Banks are urged to thoroughly assess claim investigations, especially those involving impersonation and stolen customer credentials.

NACHA OPERATING RULE AMENDMENTS FOR FRAUD MONITORING

Phase 1 – March 20, 2026: RDFIs with annual ACH receipt volume of 10 million or greater in 2023. Phase 2 – June 19, 2026: All other RDFIs.

- Financial institutions must establish and implement risk-based processes and procedures, relevant to the role it plays in the authorization or Transmission of Entries, that are reasonably intended to identify Entries that are suspected of being unauthorized or authorized under False Pretenses; and
- Review (at least annually) these processes and procedures and make appropriate updates to address evolving risks.
- For transactions that monitoring identifies as suspect, the ODFI can consider a number of actions. Actions may include, but are not limited to:
  - stopping further processing of a flagged transaction;
  - consulting with the Originator to determine the validity of the transaction;
  - consulting with other internal monitoring teams or systems to determine if the transaction raises other flags; and
  - contacting the RDFI to determine if characteristics of the Receiver's account raise additional red flags, or requesting the freeze or the return of funds.
- With respect to debits, a robust return and return rate monitoring program in conformance with existing Rules (as well as any required compliance with other specific fraud detection Rules for WEB debits and Micro-Entries) is sufficient as a minimum level of fraud monitoring.

ELDER FINANCIAL ABUSE

- **AB 909: Financial abuse of an elder or dependent adult: fraudulent transactions:** A Regulation E-like consumer protection bill that limits consumer liability and redefines "fraudulently induced transactions". Requires banks to investigate and determine within 10 business days whether a consumer is a victim, and shifts burden of proof to the banks.
- **AB 83: California Elder Financial Abuse Prevention Act:** Authorizes a depository institution to take action when, based on their own observations or information received from a governmental or law enforcement agency there is belief that the covered individual is the victim or target of financial abuse, including delaying or refusing a transaction involving the eligible adult and preventing the transfer of funds from the eligible adult's account. Also allows for notification of an "associated third party" if the eligible adult may be the victim of financial abuse, exempting the disclosure from state privacy laws or requirements.

REGULATORY RESPONSE TO EXECUTIVE ORDER ON FAIR BANKING

- OCC announcement on September 8, 2025
  - Requested information about debanking from the largest institutions
  - Updated customer complaint website
  - Reviewing customer complaint data to refine "examination efforts"
  - Reviewing approach to BSA/AML supervision to ensure it is not contributing to unlawful debanking
- Order directs the SBA to "give notice" to financial intuitions subject to the SBA's jurisdiction and supervision
  - On August 26, 2025, the SBA issued a letter that directs financial institutions to "file a detailed report"

Purpose of the Executive Order

The order aims to ensure banks do not deny services based on political or ideological beliefs.

Response to Debanking Concerns

'Debanking' concerns prompted action to address incidents where individuals or groups felt unfairly denied banking services.

OCC's Response

The Office of the Comptroller of the Currency issued announced actions being taken to address politicized or unlawful debanking.

U.S. SMALL BUSINESS ADMINISTRATION OFFICE OF
GENERAL COUNSEL
WASHINGTON, DC 20416

On August 7, 2025, President Donald J. Trump issued the Executive Order 14331, Guaranteeing Fair Banking for All Americans ("Fair Banking Executive Order"), instructing the SBA, along with federal banking regulators, to end the practice of politicized or unlawful debanking, which is the practice where banks and financial services providers, both independently and at the direction of federal regulators, freeze or close accounts, deny loans, and refuse services to "politically disfavored" people and businesses.

In connection with the Fair Banking Executive Order, and in order for your institution to maintain good standing status under 13 CFR § 120.410(e) and § 120.420(e), the SBA recently sent a letter (the "SBA Letter") requiring your institution to cease any politicized or unlawful debanking actions, attempt to reinstate affected customers, and provide a detailed report addressing and evidencing your compliance with the Executive Order.

In acknowledgment of the commitment that the Federal banking regulators[1] have demonstrated to the Fair Banking Executive Order,[2] and to ensure that community banks and other small lenders continue to focus their limited resources on lending in their communities and other community banking activities, the SBA is clarifying how an institution that has less than $30,000,000,000 in total assets as of June 30, 2025, and is supervised by any of the Federal banking regulators, may comply with the SBA's reporting requirements in the SBA Letter.[3]

Specifically, by using the enclosed form and meeting the criteria set forth therein, an institution can demonstrate compliance with the reporting requirements in the SBA Letter.

This form and any supplementary information shall be submitted to debanking@sba.gov by January 5, 2026.

Sincerely,

Wendell Davis
General Counsel, Office of the General Counsel
U.S. Small Business Administration

[1] As provided in the Fair Banking Executive Order, the term "Federal banking regulators" refers to the SBA and the Federal member agencies of the Financial Stability Oversight Council with supervisory and regulatory authority over banks, savings associations, or credit unions. Institutions supervised by SBA include SBA Supervised Lenders (as defined in 13 CFR § 120.10).
[2] *See, e.g.*, OCC News Release 2025-78, dated August 7, 2025; Statement from Acting Chairman Travis Hill on Executive Order Titled "Guaranteeing Fair Banking For All Americans", dated August 7, 2025.
[3] The term "reasonable review" for purposes of the enclosed model reporting form refers solely to efforts and reviews conducted by the institution in good faith, accounting for the institution's size, complexity, and risk profile. An institution should review readily available, existing records kept in the ordinary course of its business, and it should rely solely on existing staffing and systems without incurring any undue cost or burden. For the avoidance of doubt, institutions should not consider the model enclosed reporting form to be a formal attestation.

Date_____

VIA EMAIL debanking@sba.gov

U.S. Small Business Administration
Office of General Counsel
Washington, DC 20416

I am submitting this form on behalf of [insert institution name] ("Institution") in response to SBA's request for a report addressing and evidencing compliance with certain requirements of Executive Order 14331, Guaranteeing Fair Banking for All Americans ("Fair Banking Executive Order"). Institution had less than $30,000,000,000 in total assets as of June 30, 2025, and is supervised by a Federal banking regulator, as defined in the Fair Banking Executive Order.

Institution engaged in a reasonable review to identify debanking policies by considering whether, in the past five years:

1. It received any notice from a State or Federal banking agency identifying instances of the Institution allegedly engaging in politicized or unlawful debanking, as described in the Fair Banking Executive Order;

2. Its board of directors or senior management had received a report (e.g., as part of regular quarterly board reporting or other management information system reporting) alleging that it engaged in politicized or unlawful debanking, as described in the Fair Banking Executive Order; and

3. It had formal or informal policies or practices that required, encouraged, or otherwise influenced the institution to engage in politicized or unlawful debanking, as specified by the Fair Banking Executive Order.

Based on this reasonable review, Institution has **[not identified any debanking policies]** ***or*** **[identified debanking policies]**.

In the event that Institution identified debanking policies, include the following paragraph:

Institution engaged in a reasonable review of its and its subsidiaries' records from the past five years to identify any previous or potential clients of Institution or its subsidiaries that were denied access to financial services or payment processing services provided by Institution or any subsidiaries through a politicized or unlawful debanking action in violation of a statutory or regulatory requirement under section 7(a) of the Small Business Act or any requirement in a Standard Operating Procedures Manual or Policy Notice ("SBA Rules"). Based on that review:

- **[Institution identified no such action]**;
- **[Institution identified such actions and attaches hereto a list identifying the number of such actions and summary of all such actions with sufficient detail to allow for follow-up by the SBA with Institution, as limited by footnote 4 below ("Summary Report")]; *or***
- **[Institution identified such actions and attaches hereto (1) a Summary Report and (2) a summary of steps taken to redress any such violations of SBA Rules].**[4]

[4] The summar(ies) attached hereto do not include any confidential supervisory information or non-public OCC information. Additionally, the summar(ies) do not include any financial records or information identified with or identifiable as being derived from the financial records of a particular customer, or any other information that is prohibited by law or regulation.

READYING FOR SECTION 1071

Statutorily Required (Will Remain Unless Congress Acts)

- Business demographic status inquiry (women-owned, minority-owned, small business)
- Core application data (number, date, type, purpose, amounts, action taken)
- Geographic data (census tract)
- Financial data (gross annual revenue)
- Principal owner demographics (race, sex, ethnicity)
- Firewall protections for demographic data
- Annual Bureau reporting
- 3-year record retention
- Public data availability

Regulatory Additions (Pending)

- LGBTQI+-owned business status
- Detailed pricing information
- Narrows "financial institution" to a 100-transaction threshold
- Specific transaction exclusions (e.g., trade credit, factoring, certain leases)
- Detailed procedures for public release of data
- Safe harbor provisions for firewall rule

UPDATES IN AML/CFT AND CYBERSECURITY RISK ASSESSMENTS

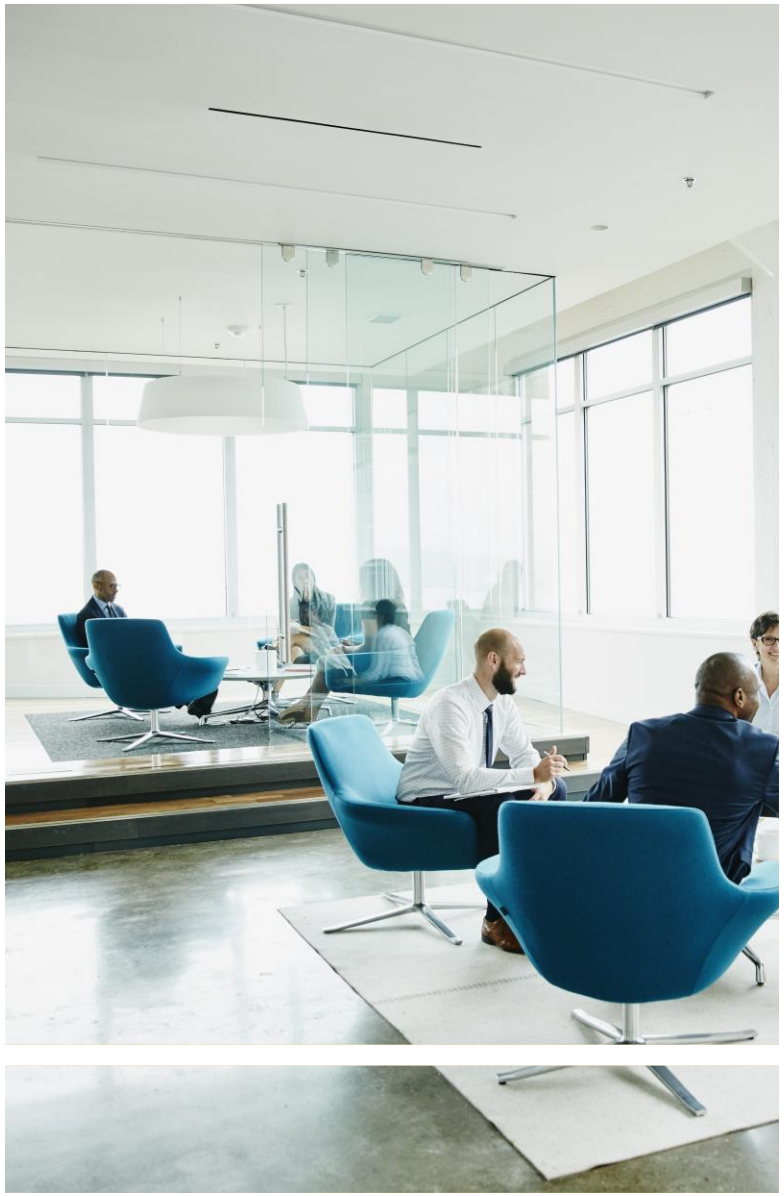
AML/CFT and Sanctions Risk Assessments

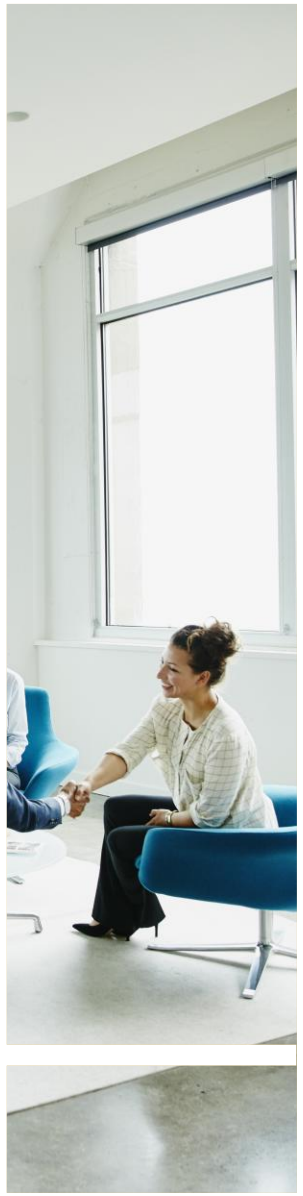
- The FFIEC examination manual indicates it is "not a specific legal requirement" but generally recommends an assessment of customers, products/services, and geographic locations
- Even though rules have not been finalized to implement the AMLA, recent enforcement actions require additional factors
  - Transactions, distribution channels, intermediaries
  - National AML/CFT Priorities

Cybersecurity Assessment Tool was Retired

- Cyber Risk Institute's (CRI) Cyber Profile
- Center for Internet Security Critical Security Controls
- National Institute of Standards and Technology (NIST) Cybersecurity Framework 2.0
- Cybersecurity and Infrastructure Security Agency's (CISA) Cybersecurity Performance Goals

ii. Periodic Risk Assessments: the extent to which TD Bank's AML program includes regular, periodic assessments of TD Bank's money laundering, terrorist financing, and other illicit financial activity risks based on TD Bank's business activities, including products, services, distribution channels, customers, intermediaries, and geographic locations.





THIRD-PARTY RISK MANAGEMENT

- Have you conducted an Artificial Intelligence Survey or review of your vendors?
- Are you looking to third parties for cryptocurrency?
- Are you managing emerging risks associated with Affinity Deposit Relationships or BaaS?
- How will you assess use of Personal Information to comply with privacy rules?
- Are third parties amenable to adding contractual language to comply with California law?
- Cybersecurity risks are increasing.

FINAL TIPS AND TAKEAWAYS

Changing Focus on Risk Assessments

- Assess AML/CFT risk assessments to ensure they include all requirements
- Migrate off the Cybersecurity Assessment Tool (if you haven't already)

Fair Banking and Interplay with BSA Examinations

- Review all policies that may include prohibited businesses (ACH, Merchant Services, BSA, Credit) and ensure you have a defensible position

Fraud Liability

- Conduct a fraud risk assessment to guide actions in 2026

Third Party Risk Management

- Determine vendors using Artificial Intelligence (AI)
- Survey for use of ADMT and how PI is collected/deleted

1. Enhance COPPA policies and technology by April 2026 to
    a. Require age verification on "mixed audience" websites
    b. Strengthen parental consent requirements through "text plus" verification
2. Evaluate applicability of ADMT, audit, and risk assessment requirements under the CCPA
    a. Implement mechanisms for ADMT consumer notice, opt-out, and access
    b. Prepare for annual audits and privacy risk assessments
    c. Amend service provider contracts for compliance assistance
    d. Monitor regulatory updates and enforcement trends

THANK YOU

Laurel Sykes, EVP, CRO

American Riviera Bank

lsykes@arb.bank

Paul Shimotake

scoutoathlaw@gmail.com